# ΚΕΦΑΛΑΙΟ 2

# Ιδεώδη και πηλικοδακτύλιοι

Τα *ιδεώδη*[1] ενός δακτυλίου $R$ είναι ειδικής φύσεως υποδακτύλιοι τού $R$ που «απορροφούν» οιαδήποτε γινόμενα στοιχείων τους με στοιχεία τού $R$ και συμπεριφέρονται «ιδεωδώς» σε ό,τι αφορά στη δόμηση *πηλικοδακτυλίων*, σε πλήρη αναλογία με ό,τι συμβαίνει με τις *ορθόθετες υποομάδες* μιας δεδομένης ομάδας.

## 2.1 ΙΔΕΩΔΗ

**2.1.1 Ορισμός.** Έστω $(R, +, \cdot)$ ένας δακτύλιος. Ένα υποσύνολο $\varnothing \neq I \subseteq R$, για το οποίο το ζεύγος $(I, +)$ αποτελεί μια υποομάδα τής προσθετικής ομάδας $(R, +)$, καλείται

• **αριστερό ιδεώδες** όταν $ra \in I$ για κάθε $r \in R$ και κάθε $a \in I$,

• **δεξιό ιδεώδες** όταν $ar \in I$ για κάθε $r \in R$ και κάθε $a \in I$,και

• **αμφίπλευρο ιδεώδες** ή απλώς **ιδεώδες** εάν το $I$ είναι συγχρόνως και αριστερό και δεξιό ιδεώδες.

**2.1.2 Παρατήρηση.** (i) Κάθε (αριστερό, δεξιό ή αμφίπλευρο) ιδεώδες ενός δακτυλίου είναι υποδακτύλιος αυτού. Ωστόσο, υπάρχουν υποδακτύλιοι δακτυλίων που δεν είναι ιδεώδη τους. (Βλ., π.χ., 2.1.4 (ii).)

[1] Το 1847 ο Ernst Eduard Kummer (1810-1893) εισήγαγε «ιδεώδεις μιγαδικούς αριθμούς» στην προσπάθειά του να διατηρήσει την ιδιότητα τής μονοσήμαντης παραγοντοποιήσεως σε κάποιους δακτυλίους αλγεβρικών αριθμών. Ωστόσο, ήταν ο Richard Dedekind (1831-1916) και η Emmy Noether (1882-1935) αυτοί που εγκαινίασαν την χρήση «ιδεωδών» ως ειδικούς υποδακτυλίους και μετεξέλιξαν τη όλη θεωρία τους, ούτως ώστε ο λογισμός με αυτά να καταστεί ένα από τα πιο απαραίτητα τεχνικά βοηθήματα των σύγχρονων αλγεβριστών.

(ii) Σε μεταθετικούς δακτυλίους οι έννοιες αριστερό, δεξιό και αμφίπλευρο ιδεώδες ταυτίζονται.

**2.1.3 Πρόταση.** *Έστω $(R,+,\cdot)$ ένας δακτύλιος. Ένα μη κενό υποσύνολο $I$ τού $R$ είναι ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες εάν και μόνον εάν ισχύουν τα εξής:*

(i) $a-b \in I$, *για οιαδήποτε* $a,b \in I$.

(ii) $ra \in I$ *(και αντιστοίχως,* $ar \in I \;/\; ra, ar \in I$*) για οιαδήποτε* $a \in I,\ r \in R$.

Απόδειξη. Προφανώς η (i) ισοδυναμεί με το ότι το ζεύγος $(I,+)$ αποτελεί μια υποομάδα τής προσθετικής ομάδας $(R,+)$ τού δακτυλίου $(R,+,\cdot)$. $\square$

**2.1.4 Παραδείγματα.** (i) Για κάθε ακέραιο $n$ η κυκλική υποομάδα

$$n\mathbb{Z} = \{nk \quad | \, k \in \mathbb{Z}\}$$

τής $(\mathbb{Z},+)$ αποτελεί ένα ιδεώδες τού δακτυλίου $(\mathbb{Z},+,\cdot)$.

(ii) Ο υποδακτύλιος $\mathbb{Z}$ τού $\mathbb{Q}$ *δεν είναι* (ούτε δεξιό ούτε αριστερό ούτε αμφίπλευρο) ιδεώδες τού $\mathbb{Q}$, διότι π.χ. $\frac{1}{2} \in \mathbb{Q}$ και $7 \in \mathbb{Z}$, αλλά $\frac{1}{2}\cdot 7 = 7 \cdot \frac{1}{2} \notin \mathbb{Z}$.

(iii) Ορίζουμε τα

$$I := \left\{ \left. \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right| \, a,b \in \mathbb{R} \right\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R})$$

και

$$J := \left\{ \left. \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \right| \, a,b \in \mathbb{R} \right\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

Το $I$ είναι δεξιό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$, διότι για οιουσδήποτε $a,b,a',b' \in \mathbb{R}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & 0 \end{pmatrix} \in I$$

και για οιουσδήποτε $a,b,c,d,e,f \in \mathbb{R}$,

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ca+eb & ad+bf \\ 0 & 0 \end{pmatrix} \in I.$$

Ωστόσο, το $I$ δεν είναι αριστερό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$, διότι π.χ.

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I.$$

Κατ' αναλογίαν, αποδεικνύεται ότι το $J$ είναι ένα αριστερό, μη δεξιό ιδεώδες τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$.

(iv) Κάθε δακτύλιος $R$ έχει πάντοτε τον εαυτό του και το $\{0_R\}$ ως ιδεώδη του. Το $\{0_R\}$ λέγεται **τετριμμένο**[2] **(ή μηδενικό) ιδεώδες**, ενώ κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες $I$ τού $R$ με $I \subsetneqq R$ λέγεται **γνήσιο** *(αριστερό/δεξιό/αμφίπλευρο)* **ιδεώδες**.

(v) Εάν ο $R$ είναι ένας δακτύλιος και $a \in R$, τότε είναι προφανές ότι το σύνολο

$$\boxed{Ra := \{ra \mid r \in R\}}$$

είναι ένα αριστερό και το σύνολο

$$\boxed{aR := \{ar \mid r \in R\}}$$

ένα δεξιό ιδεώδες τού $R$.

(vi) Έστω $R$ ένας δακτύλιος και έστω $S \subsetneqq R$ ένας γνήσιος υποδακτύλιός του. Θεωρούμε ένα μη κενό υποσύνολο $I \subseteq S$. Εάν το $I$ είναι ένα (αριστερό/ δεξιό/ αμφίπλευρο) ιδεώδες τού $R$, τότε το $I$ είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού $S$. Αντιθέτως, εάν το $I$ είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού $S$, τότε το $I$ δεν είναι κατ' ανάγκην ένα ομοειδές ιδεώδες τού $R$. Επί παραδείγματι, εάν $R := \mathrm{Mat}_{2\times 2}(\mathbb{R})$ και

$$I := \left\{ \left. \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} \right| s \in \mathbb{R} \right\} \subsetneqq \left\{ \left. \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right| a, b, c \in \mathbb{R} \right\} =: S \subsetneqq R,$$

τότε το $I$ είναι ένα (αμφίπλευρο) ιδεώδες τού $S$, διότι για $a, b, c, s, s' \in \mathbb{R}$ έχουμε

$$\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & s' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & s - s' \\ 0 & 0 \end{pmatrix} \in I$$

και

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & as \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & s \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & sc \\ 0 & 0 \end{pmatrix} \in I.$$

Από την άλλη μεριά, το $I$ δεν είναι (αμφίπλευρο) ιδεώδες τού $R$, διότι π.χ.

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin I.$$

**2.1.5 Πρόταση.** *Έστω $\{I_\lambda \mid \lambda \in \Lambda\}$ μια οικογένεια αριστερών (και αντιστοίχως, δεξιών/αμφιπλεύρων) ιδεωδών ενός δακτυλίου $R$. Τότε η τομή $\bigcap_{\lambda \in \Lambda} I_\lambda$ των μελών της αποτελεί ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού $R$.*

[2] Προσοχή! Ορισμένοι συγγραφείς (την ορολογία των οποίων δεν ακολουθούμε εν προκειμένω) χαρακτηρίζουν ως *τετριμμένα ιδεώδη* ενός δακτυλίου $R$ *αμφότερα* τα $\{0_R\}$ και $R$.

ΑΠΟΔΕΙΞΗ. Εάν η $\{I_\lambda \mid \lambda \in \Lambda\}$ μια οικογένεια αριστερών (και αντιστοίχως, δεξιών/αμφιπλεύρων) ιδεωδών ενός δακτυλίου $R$, και $r \in R$, $a, b \in \bigcap\limits_{\lambda \in \Lambda} I_\lambda$, τότε

$$(a, b \in I_\lambda,\ \forall\, \lambda \in \Lambda) \underset{[I_\lambda \text{ ιδεώδες}]}{\Longrightarrow} \left\{ \begin{array}{l} a - b \in I_\lambda \\ ra \text{ (αντ., } ar \in I_\lambda \ / \ ra, ar \in I_\lambda) \\ \forall\, \lambda \in \Lambda \end{array} \right\},$$

οπότε και η τομή $\bigcap\limits_{\lambda \in \Lambda} I_\lambda$ αποτελεί ένα αριστερό (και αντιστοίχως, ένα δεξιό/ αμφίπλευρο) ιδεώδες τού $R$. □

**2.1.6 Πρόταση.** *Έστω $R$ ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το $I$ είναι ένα γνήσιο (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού $R$, τότε το $I$ δεν περιέχει κανένα (εξ αριστερών/ εκ δεξιών / αμφιπλεύρως) αντιστρέψιμο στοιχείο τού $R$.*

ΑΠΟΔΕΙΞΗ. Εάν το $I$ είναι ένα γνήσιο (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού $R$ και εάν υποθέσουμε ότι υπάρχει κάποιο $a \in I \smallsetminus \{0_R\}$, ούτως ώστε να ισχύει

$$ba = 1_R \quad (\text{αντ., } ab = 1_R \ / \ ab = ba = 1_R)\,,$$

για κάποιο $b \in R \smallsetminus \{0_R\}$, τότε από τον ορισμό ενός (αριστερού/ δεξιού/ αμφιπλεύρου) ιδεώδους είναι πρόδηλο ότι και τα γινόμενα αυτά (που ισούνται με $1_R$) οφείλουν να ανήκουν στο $I$. Άρα

$$1_R \in I \Longrightarrow [\forall r \in R : r \cdot 1_R = r \in I, \text{ αντ., } 1_R \cdot r = r] \Longrightarrow I = R,$$

πράγμα που έχουμε εκ των προτέρων αποκλείσει. □

**2.1.7 Πόρισμα.** *Έστω $R$ ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το $I$ είναι ένα γνήσιο (αριστερό/ δεξιό/ αμφίπλευρο) ιδεώδες τού $R$, τότε το $I$ δεν περιέχει το $1_R$.*

**2.1.8 Πρόταση.** *Έστω $R$ ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο $R$ είναι διαιρετικός δακτύλιος.*

(ii) *Τα μόνα αριστερά ιδεώδη τού $R$ είναι το $\{0_R\}$ και ο ίδιος ο $R$.*

(iii) *Τα μόνα δεξιά ιδεώδη τού $R$ είναι το $\{0_R\}$ και ο ίδιος ο $R$.*

ΑΠΟΔΕΙΞΗ. (i)⇔(ii) Εάν ο $R$ είναι διαιρετικός δακτύλιος και το $\{0_R\} \subsetneqq I \subseteq R$ ένα αριστερό ιδεώδες αυτού, τότε υπάρχει κάποιο $a \in I \smallsetminus \{0_R\}$. Εξ ορισμού, το $a$ διαθέτει αντίστροφο $a^{-1}$. Επειδή $1_R = a^{-1}a \in I$, έχουμε $I = R$. Και αντιστρόφως·

υποθέτοντας ότι τα μόνα αριστερά ιδεώδη τού $R$ είναι το $\{0_R\}$ και ο ίδιος ο $R$, και θεωρώντας οιοδήποτε στοιχείο $a \in R \smallsetminus \{0_R\}$ και το αριστερό, μη τετριμμένο ιδεώδες $Ra$ τού $R$, παρατηρούμε ότι

$$1_R \in R = Ra \Longrightarrow \exists b \in R \smallsetminus \{0_R\} : ba = 1_R,$$

ήτοι ότι το στοιχείο $a$ διαθέτει κάποιο εξ αριστερών αντίστροφο στοιχείο $b$. Επειδή $b \in R \smallsetminus \{0_R\}$, επαναλαμβάνοντας την ανωτέρω επιχειρηματολογία για το $b$ συμπεραίνουμε ότι

$$1_R \in R = Rb \Longrightarrow \exists c \in R \smallsetminus \{0_R\} : cb = 1_R,$$

ήτοι ότι το $b$ διαθέτει κάποιο εξ αριστερών αντίστροφο στοιχείο $c$. Επειδή το $b$ έχει το $a$ ως εκ δεξιών αντίστροφό του στοιχείο, έχουμε κατ' ανάγκην $a = c$ (βλ. πρόταση 1.2.8) και $ab = 1_R = ba \Longrightarrow a \in R^\times$, οπότε ο $R$ είναι διαιρετικός δακτύλιος. Η ισοδυναμία (i)⇔(iii) αποδεικνύεται παρομοίως. □

**2.1.9 Πόρισμα.** *Τα μόνα αμφίπλευρα ιδεώδη ενός διαιρετικού δακτυλίου $R$ είναι το $\{0_R\}$ και ο ίδιος ο $R$.*

**2.1.10 Παρατήρηση.** Υπάρχουν *μη μεταθετικοί, μη διαιρετικοί* δακτύλιοι $R$, όπως είναι ο $R = \mathrm{Mat}_{2\times 2}(\mathbb{R})$ (βλ. πρόταση 2.3.4), οι οποίοι δεν διαθέτουν άλλα αμφίπλευρα ιδεώδη πέραν των $\{0_R\}$ και $R$.

**2.1.11 Πόρισμα.** *Έστω $R$ ένας μη τετριμμένος, μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε ο $R$ είναι σώμα εάν και μόνον εάν τα μόνα αμφίπλευρα ιδεώδη του είναι το $\{0_R\}$ και ο ίδιος ο $R$.*

## 2.2 ΙΔΕΩΔΗ ΠΑΡΑΓΟΜΕΝΑ ΑΠΟ ΣΥΝΟΛΑ

Μια συνήθης μέθοδος κατασκευής ιδεωδών ενός δοθέντος δακτυλίου είναι η κατά φυσικό τρόπο «παραγωγή τους» από τυχόντα υποσυνόλα τού δακτυλίου.

**2.2.1 Ορισμός.** Έστω $(R, +, \cdot)$ ένας δακτύλιος και έστω $A \subseteq R$. Τότε η τομή

$$\boxed{\langle A \rangle := \bigcap \{ \text{ιδεώδη } I \text{ τού } R \mid I \supseteq A\}}$$

των μελών τής οικογενείας όλων των ιδεωδών αυτού, τα οποία περιέχουν το $A$, καλείται **το ιδεώδες το παραγόμενο από το** $A$ ή το ιδεώδες **με γεννήτορες** τα στοιχεία τού $A$. Όταν $A = \varnothing$, τότε $\langle A \rangle = \{0_R\}$. Όταν το $A = \{a_1, \ldots, a_k\}$ είναι πεπερασμένο, τότε το ιδεώδες $\langle A \rangle$ λέγεται **πεπερασμένως παραγόμενο** και συμβολίζεται απλούστερα ως $\langle a_1, \ldots, a_k \rangle$. Ένα ιδεώδες παραγόμενο από ένα και μόνον στοιχείο τού $R$ καλείται **κύριο ιδεώδες**.

**2.2.2 Πρόταση.** *Έστω $R$ ένας δακτύλιος και έστω $\varnothing \neq A \subseteq R$.*

(i) *Το ιδεώδες $\langle A \rangle$ το παραγόμενο από το $A$ αποτελείται από όλα τα στοιχεία τής μορφής*

$$\sum_{i=1}^{\kappa} r_i a_i s_i + \sum_{j=1}^{\mu} r'_j a'_j + \sum_{k=1}^{\nu} a''_k s''_k + \sum_{\varrho=1}^{\xi} n_\varrho a'''_\varrho \tag{2.1}$$

$r_i, s_i, r'_j, s''_k \in R, \quad a_i, a'_j, a''_k, a'''_\varrho \in A \quad$ *και* $\quad n_\varrho \in \mathbb{Z},$

$$\forall i \in \{1, ..., \kappa\}, \quad \forall j \in \{1, ..., \mu\}, \quad \forall k \in \{1, ..., \nu\}, \quad \forall \varrho \in \{1, ..., \xi\},$$

*όπου $\kappa, \mu, \nu, \xi$ είναι θετικοί ακέραιοι αριθμοί.*

(ii) *Εάν ο $R$ είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle A \rangle = \left\{ \sum_{i=1}^{\kappa} r_i \, a_i \, s_i \;\middle|\; r_1, \ldots, r_\kappa, s_1, \ldots, s_\kappa \in R, \; a_1, ..., a_\kappa \in A, \quad \kappa \in \mathbb{N} \right\} .$$

(iii) *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος, τότε*

$$\langle A \rangle = \left\{ \sum_{i=1}^{\kappa} r_i \, a_i \; + \sum_{\varrho=1}^{\xi} n_\varrho a'_\varrho \;\middle|\; \begin{array}{c} r_1, \ldots, r_\kappa \in R, \quad n_1, \ldots, n_\xi \in \mathbb{Z}, \\ a_1, ..., a_\kappa, a'_1, ..., a'_\xi, \in A, \quad \kappa, \xi \in \mathbb{N} \end{array} \right\} .$$

(iv) *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle A \rangle = \left\{ \sum_{i=1}^{\kappa} r_i \, a_i \;\middle|\; r_1, \ldots, r_\kappa \in R, \; a_1, \ldots, a_\kappa \in A, \; \kappa \in \mathbb{N} \right\} .$$

ΑΠΟΔΕΙΞΗ. (i) Έστω $I$ το υποσύνολο τού $R$ το απαρτιζόμενο από όλα τα στοιχεία τής μορφής (2.1). Τόσο η διαφορά δυο στοιχείων τής μορφής (2.1) όσο και το γινόμενο ενός $r \in R$ με οιοδήποτε στοιχείο τής μορφής (2.1) είναι και πάλι τής μορφής (2.1). Άρα το $I$ είναι ένα ιδεώδες τού $R$ που περιέχει το $A$ (αφού -λόγω τού τελευταίου αθροίσματος- $1_{\mathbb{Z}} a = a \in I$, για κάθε $a \in A$). Κατά συνέπειαν, $\langle A \rangle \subseteq I$. Και αντιστρόφως· κάθε ιδεώδες που περιέχει το $A$ οφείλει να περιέχει και τα αθροίσματα τής μορφής (2.1), οπότε έχουμε $I \subseteq \langle A \rangle$.

(ii) Εάν ο $R$ είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε τα αθροίσματα τής μορφής (2.1) μπορούν να «συμπτυχθούν» (κατά τα αναγραφόμενα), αφού

$$r\, a = r\, a\, 1_R, \quad a\, s = a\, s\, 1_R, \; \forall a \in A, \; \forall\, (r, s) \in R \times R,$$

και

$$na = n\,(1_R\, a) = (n\, 1_R)\,(a\, 1_R)\,, \quad \forall n \in \mathbb{Z}, \; \forall a \in A.$$

(iii) Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος, τότε τα αθροίσματα τής μορφής (2.1) μπορούν και πάλι να «συμπτυχθούν» (κατά τα αναγραφόμενα), αφού

$$ras = (rs)a, \ ra = ar, \ \ \forall a \in A, \ \ \forall\,(r,s) \in R \times R.$$

(iv) Τέλος, εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε ενσωματώνουμε στο $\langle A \rangle$ και τα δύο είδη «συμπτύξεων» τής μορφής των στοιχείων που περιγράψαμε προηγουμένως στα (ii) και (iii). □

**2.2.3 Σημείωση.** Εάν ο $R$ είναι ένας δακτύλιος και $A \subseteq R$, τότε μπορεί κανείς να ορίσει και τα δεξιά/αριστερά ιδεώδη

$$\langle A \rangle_{\text{αρ}} := \bigcap \{ \text{ αριστερά ιδεώδη } I \ \text{ τού } \ R \mid I \supseteq A \}$$

και

$$\langle A \rangle_{\delta} := \bigcap \{ \text{ δεξιά ιδεώδη } I \ \text{ τού } \ R \mid I \supseteq A \},$$

αντιστοίχως, τα παραγόμενα από το $A$, και να αποδείξει τις ιδιότητές τους που αναλογούν σε αυτές που προαναφέρθηκαν στην πρόταση 2.2.2 για το $\langle A \rangle$.

**2.2.4 Πόρισμα.** *Έστω ότι ο $R$ είναι ένας δακτύλιος και ότι $a \in R$.*

(i) *Το κύριο ιδεώδες $\langle a \rangle$ αποτελείται από όλα τα στοιχεία τής μορφής*

$$\sum_{j=1}^{k} r_j \, a \, s_j + r\,a + a\,s + n\,a,$$

$r, s, r_1, \ldots, r_k, s_1, \ldots, s_k \in R, \ k \in \mathbb{N}$ *και* $n \in \mathbb{Z}$.

(ii) *Εάν ο $R$ είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle a \rangle = \left\{ \sum_{j=1}^{k} r_j \, a \, s_j \ \middle| \ r_1, \ldots, r_k, s_1, \ldots, s_k \in R, \ k \in \mathbb{N} \right\}.$$

(iii) *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος, τότε*

$$\langle a \rangle = \{ r\,a + n\,a \mid r \in R, \ n \in \mathbb{Z} \}.$$

(iv) *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε*

$$\langle a \rangle = Ra = \{ r\,a \mid r \in R \}.$$

**2.2.5 Παρατήρηση.** Όταν ο $R$ είναι μεταθετικός αλλά *δεν* διαθέτει μοναδιαίο στοιχείο και $a \in R$, τα ιδεώδη του $\langle a \rangle$ και $Ra$ *δεν* είναι κατ' ανάγκην ίσα. Επί παραδείγματι, όταν $R = 2\mathbb{Z}$, τότε $\langle 2 \rangle \neq (2\mathbb{Z})\,2$, διότι $2 \in \langle 2 \rangle$, ενώ $2 \notin (2\mathbb{Z})\,2$.

**2.2.6 Πρόταση.** *Κάθε ιδεώδες τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών είναι τής μορφής $\langle n \rangle = n\mathbb{Z}$, όπου $n \in \mathbb{Z}$. (Οι εν λόγω γεννήτορες $n$ είναι, βεβαίως, δυνατόν να περιορισθούν στα στοιχεία τού συνόλου $\mathbb{N}_0$, καθότι μια ενδεχόμενη αλλαγή προσήμου τού εκάστοτε θεωρούμενου $n$ δεν επιφέρει διαφοροποίηση τού κυρίου ιδεώδους $\langle n \rangle$.) Ως εκ τούτου, κάθε ιδεώδες τού δακτυλίου $\mathbb{Z}$ είναι κύριο ιδεώδες.*

ΑΠΟΔΕΙΞΗ. Έστω $I$ ένα ιδεώδες τού $\mathbb{Z}$. Εάν $I = \{0\}$, τότε $I = \langle 0 \rangle$. Εάν $\{0\} \subsetneqq I$, τότε υπάρχει κάποιος ακέραιος $n \in I \setminus \{0\}$. Άρα και ο αντίθετός του ανήκει στο $I \setminus \{0\}$ (αφού $-n = 0 - n$ με $0 \in I$ και $n \in I$). Ως εκ τούτου, *κάθε* μη τετριμμένο ιδεώδες $I$ τού $\mathbb{Z}$ περιέχει *θετικούς ακεραίους*. Έστω

$$n_0 := \min\{ n \in \mathbb{N} \mid n \in I \}.$$

Θα δείξουμε ότι $I = \langle n_0 \rangle$. Πράγματι· έστω $a$ τυχόν στοιχείο τού $I$. Τότε το $a$ διαιρούμενο με το $n_0$ δίνει υπόλοιπο $r$, όπου

$$a = n_0 q + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < n_0,$$

οπότε

$$q \in \mathbb{Z},\ n_0 \in I \Longrightarrow n_0 q \in I \underset{a \in I}{\Longrightarrow} a - n_0 q = r \in I,$$

απ' όπου έπεται ότι $r = 0$ (διότι αλλιώς θα παρουσιαζόταν αντίφαση ως προς την επιλογή τού $n_0$). Άρα $a = n_0 q \in \langle n_0 \rangle$, ήτοι $I \subseteq \langle n_0 \rangle$. Από την άλλη μεριά,

$$\langle n_0 \rangle = \{ k n_0 \mid k \in \mathbb{Z} \} \subseteq I.$$

Άρα τελικώς $I = \langle n_0 \rangle = \langle -n_0 \rangle$. □

## 2.3 ΔΑΚΤΥΛΙΟΙ ΜΕ «ΛΙΓΑ» ΙΔΕΩΔΗ

Υπάρχουν δακτύλιοι με *μικρό αριθμό ιδεωδών*, οι οποίοι αξίζουν ιδιαίτερης μνείας.

**2.3.1 Ορισμός.** Ένας μη τετριμμένος δακτύλιος $R$ ονομάζεται **απλός δακτύλιος** όταν δεν διαθέτει (αμφίπλευρα) ιδεώδη πέραν τού $\{0_R\}$ και τού $R$.[3].

**2.3.2 Πρόταση.** *Κάθε διαιρετικός δακτύλιος είναι απλός.*

ΑΠΟΔΕΙΞΗ. Άμεση συνέπεια τού πορίσματος 2.1.11. □

[3] Ο εν λόγω ορισμός είναι ανάλογος εκείνου των *απλών ομάδων*.

**2.3.3 Πρόταση.** *Ένας μη τετριμμένος μεταθετικός δακτύλιος $R$ με μοναδιαίο στοιχείο είναι σώμα εάν και μόνον εάν είναι απλός.*

ΑΠΟΔΕΙΞΗ. Άμεση συνέπεια τού πορίσματος 2.1.9. □

**2.3.4 Πρόταση.** *Εάν ο $R$ είναι ένας διαιρετικός δακτύλιος και $n \in \mathbb{N}$, τότε ο $\mathrm{Mat}_{n\times n}(R)$ είναι ένας απλός δακτύλιος.*

ΑΠΟΔΕΙΞΗ. Έστω $I$ ένα ιδεώδες τού $\mathrm{Mat}_{n\times n}(R)$ διάφορο τού τετριμμένου. Τότε υπάρχει ένας πίνακας

$$\mathbf{A} = (a_{jk})_{1\leq j,k\leq n} \in I\setminus\{0_{\mathrm{Mat}_{n\times n}(R)}\},$$

οπότε υπάρχουν $j_0, k_0 \in \{1, ..., n\}$ με $a_{j_0k_0} \neq 0_R$. Έστω ότι ο $\mathbf{E}_{jk} \in \mathrm{Mat}_{n\times n}(R)$ είναι ο βοηθητικός πίνακας, ο οποίος έχει ως εγγραφή του στη θέση $(j,k)$ το $1_R$ και σε όλες τις άλλες θέσεις εγγραφές που ισούνται με το $0_R$. Τότε για κάθε δείκτη $l \in \{1, 2, ..., n\}$ λαμβάνουμε[4]

$$\mathbf{E}_{lj_0}\,\mathbf{A}\,\mathbf{E}_{k_0l} = a_{j_0k_0}\mathbf{E}_{ll}.$$

Επειδή $\mathbf{A} \in I$ και $\mathbf{E}_{lj_0}, \mathbf{E}_{k_0l} \in \mathrm{Mat}_{n\times n}(R)$, τούτο σημαίνει ότι $a_{j_0k_0}\mathbf{E}_{ll} \in I$. Επιπροσθέτως, επειδή ο $R$ είναι διαιρετικός δακτύλιος, ορίζεται το αντίστροφο στοιχείο $a_{j_0k_0}^{-1}$ τού $a_{j_0k_0}$. Ως εκ τούτου,

$$\left.\begin{array}{l} a_{j_0k_0}\mathbf{E}_{ll} \in I, \\ a_{j_0k_0}^{-1}\mathbf{E}_{ll} \in \mathrm{Mat}_{n\times n}(R) \end{array}\right\} \Longrightarrow (a_{j_0k_0}\mathbf{E}_{ll})\left(a_{j_0k_0}^{-1}\mathbf{E}_{ll}\right) = \mathbf{E}_{ll} \in I,$$

απ' όπου έπεται ότι

$$\mathbf{I}_n := \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix} = \sum_{l=1}^{n} \mathbf{E}_{ll} \in I.$$

Επειδή το μοναδιαίο στοιχείο $\mathbf{I}_n$ τού $\mathrm{Mat}_{n\times n}(R)$ ανήκει στο ιδεώδες $I$, έχουμε κατ' ανάγκην $I = \mathrm{Mat}_{n\times n}(R)$. □

**2.3.5 Πρόταση.** *Κάθε ακεραία περιοχή $R$, η οποία διαθέτει μόνον έναν πεπερασμένο αριθμό ιδεωδών, είναι σώμα.*

[4] Ο πίνακας $a_{j_0k_0}\mathbf{E}_{ll}$ δηλοί *αριθμητικό πολλαπλασιασμό* τού $\mathbf{E}_{ll}$ με τον $a_{j_0k_0}$ και είναι -ως εκ τούτου- ο πίνακας που έχει ως εγγραφή του στη θέση $(l,l)$ το $a_{j_0k_0}$ και σε όλες τις άλλες θέσεις εγγραφές που είναι ίσες με το $0_R$.

ΑΠΟΔΕΙΞΗ. Έστω $a \in R \smallsetminus \{0_R\}$. Θεωρούμε τα κύρια ιδεώδη $\langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \ldots$ Επειδή

$$\left[a^{k+1} = aa^k \in \left\langle a^k \right\rangle, \ \forall k \in \mathbb{N}\right] \Longrightarrow \left[\left\langle a^{k+1} \right\rangle \subseteq \left\langle a^k \right\rangle, \ \forall k \in \mathbb{N}\right],$$

σχηματίζεται η εξής ακολουθία διαδοχικώς εγκλειομένων κυρίων ιδεωδών:

$$\langle a \rangle \supseteq \left\langle a^2 \right\rangle \supseteq \left\langle a^3 \right\rangle \supseteq \cdots$$

Επειδή η ακεραία περιοχή $R$ διαθέτει μόνον έναν πεπερασμένο αριθμό ιδεωδών, θα υπάρχει κάποιος $n \in \mathbb{N}$, τέτοιος ώστε

$$\langle a^n \rangle = \left\langle a^{n+1} \right\rangle \Longrightarrow \left[(\exists r \in R) : a^n = ra^{n+1}\right].$$

Όμως τούτο έχει ως συνέπεια ότι $a^n(1_R - ra) = 0_R$, το οποίο, συνδυαζόμενο με το ότι $a^n \in R \smallsetminus \{0_R\}$ και το ότι ο $R$ είναι εξ υποθέσεως ακεραία περιοχή, μας δίδει $ra = 1_R$, οπότε το $r$ είναι (πολλαπλασιαστικό) αντίστροφο τού (αυθαιρέτως επιλεγμένου) μη μηδενικού στοιχείου $a$. $\square$

## 2.4 ΛΟΓΙΣΜΟΣ ΜΕ ΙΔΕΩΔΗ

Τα ιδεώδη ενός δακτυλίου μπορούν να προστεθούν, να πολλαπλασιασθούν ή -σε ορισμένες περιπτώσεις- 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.

**2.4.1 Ορισμός.** Έστω ότι ο $R$ είναι ένας δακτύλιος και τα $I_1, \ldots, I_n$, $n \in \mathbb{N}$, $n \geq 2$, αριστερά (και αντιστοίχως, δεξιά/αμφίπλευρα) ιδεώδη του. Ορίζουμε το **άθροισμα** και το **γινόμενό** τους ως:

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

και

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

αντιστοίχως. Είναι εύκολο να διαπιστωθεί ότι τόσο το $I_1 + \cdots + I_n$ όσο και το $I_1 \cdots I_n$ αποτελεί ένα αριστερό (και αντιστοίχως, ένα δεξιό/αμφίπλευρο) ιδεώδες τού $R$.

**2.4.2 Σημείωση.** (i) Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου $R$ με μοναδιαίο στοιχείο, τότε

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

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

$$\left\{ \sum_{i=1}^{\kappa} r_i\, a_i\, s_i \;\middle|\; r_1, \ldots, r_\kappa, s_1, \ldots, s_\kappa \in R,\ a_1, ..., a_\kappa \in I_1 \cup \cdots \cup I_n,\ \ \kappa \in \mathbb{N} \right\},$$

κάθε $x \in \langle I_1 \cup \cdots \cup I_n \rangle$ μπορεί (ενδεχομένως ύστερα από κάποια αναδιάταξη δεικτών) να γραφεί υπό τη μορφή $x = x_1 + x_2 + \cdots + x_n$, όπου για κάθε $j \in \{1, \ldots, n\}$,

$$x_j = \sum_{i=1}^{\kappa_j} r_i\, a_i\, s_i,\ \ r_1, \ldots, r_{\kappa_j}, s_1, \ldots, s_{\kappa_j} \in R,$$

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

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

(ii) 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 $3\mathbb{Z} \cup 5\mathbb{Z}$, αλλ' εντούτοις

$$2 = 5 - 3 \notin 3\mathbb{Z} \cup 5\mathbb{Z}.$$

(iii) 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 ακολουθία διαδοχικώς εγκλειομένων 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 (πρβλ. 2.4.13 (iii)), έχουμε

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

Οι προτάσεις 2.4.3, 2.4.4, 2.4.5 και 2.4.14, οι οποίες ακολουθούν, έχουν ως στόχο την περιγραφή ορισμένων βασικών αρχών τού «λογισμού με ιδεώδη».

**2.4.3 Πρόταση.** *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a, b \in R$, τότε*

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

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

ΑΠΟΔΕΙΞΗ. (i) Επειδή έχουμε $\langle a \rangle = Ra$ και $\langle b \rangle = Rb$, τούτο έπεται άμεσα από το 2.4.2 (i).

(ii) Προφανώς,

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

όπου $Rab = \langle ab \rangle$. □

**2.4.4 Πρόταση.** *Έστω ότι ο $R$ είναι ένας δακτύλιος και $I_1, I_2, I_3, I_3'$ τέσσερα (αριστερά, δεξιά ή αμφίπλευρα) ιδεώδη του. Τότε ισχύουν τα εξής:*

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

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

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

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

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

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

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

Κατά συνέπειαν, $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$.

(ii) Έστω τυχόν $x \in (I_1\, I_2)\, I_3$. Τότε

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

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

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

Επομένως, λόγω τής επιμεριστικής ιδιότητας,

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

Αναλόγως αποδεικνύεται και η εγκλειστική σχέση $I_1\ (I_2\, I_3) \subseteq (I_1\, I_2)\ I_3$.

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας,

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

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

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

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

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

ΑΠΟΔΕΙΞΗ. (i) Εάν $x \in I_1\, I_2$, τότε

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

Όμως, από τον ορισμό τού ιδεώδους,

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

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

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

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

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

**2.4.6 Σημείωση.** Οι εγκλεισμοί (i) και (ii) τής προτάσεως 2.4.5 μπορούν να είναι αυστηροί ακόμη και για μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο. Επί παραδείγματι, εάν εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών θεωρήσουμε τα ιδεώδη $I_1, I_2$, με $I_1 = I_2 := \langle 2 \rangle$, τότε

$$I_1\, I_2 = \langle 4 \rangle \subsetneqq I_1 \cap I_2 = \langle 2 \rangle .$$

Επίσης, για τα ιδεώδη $I_1 := \langle 12 \rangle, I_2 := \langle 20 \rangle, I_3 := \langle 30 \rangle$ έχουμε

$$(I_1 + I_2)\,(I_1 + I_3) = \langle 24 \rangle \subsetneqq I_1 + I_2\, I_3 = \langle 12 \rangle$$

και για τα ιδεώδη $I_1 := \langle 24 \rangle, I_2 := \langle 4 \rangle, I_3 := \langle 6 \rangle$ έχουμε

$$I_1 + I_2\, I_3 = \langle 24 \rangle \subsetneqq I_1 + (I_2 \cap I_3) = \langle 12 \rangle$$

(πρβλ. πόρισμα 2.4.13).

**2.4.7 Πρόταση.** *Έστω ότι ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και τα $I_1, I_2$ δυο ιδεώδη του με $I_1 + I_2 = R$. Τότε*

$$I_1\, I_2 = I_1 \cap I_2.$$

ΑΠΟΔΕΙΞΗ. Κατά το (i) τής προτάσεως 2.4.5, $I_1\, I_2 \subseteq I_1 \cap I_2$. Έστω τυχόν στοιχείο $a \in I_1 \cap I_2$. Επειδή $I_1 + I_2 = R$, υπάρχουν $b \in I_1$ και $c \in I_2$, τέτοια ώστε να ισχύει η ισότητα $b + c = 1_R$, οπότε

$$\left.\begin{array}{r} a = a \cdot 1_R = a(b + c) = ab + ac \\ a \in I_2, b \in I_2 \Rightarrow ab \in I_2\, I_1 = I_1\, I_2 \\ a \in I_1, c \in I_2 \Rightarrow ac \in I_1\, I_2 \end{array}\right\} \Longrightarrow a \in I_1\, I_2,$$

απ’ όπου έπεται και ο αντίστροφος εγκλεισμός $I_1 \cap I_2 \subseteq I_1\, I_2$. □

**2.4.8 Ορισμός.** Κάθε ιδεώδες $I$ ενός δακτυλίου $R$, για το οποίο

$$\exists n \in \mathbb{N} : I^n = \{0_R\},$$

καλείται **μηδενοδύναμο ιδεώδες**.

**2.4.9 Πρόταση.** *Κάθε στοιχείο ενός μηδενοδύναμου ιδεώδους $I$ ενός δακτυλίου $R$ είναι μηδενοδύναμο στοιχείο τού $R$* (βλ. 1.2.15), *δηλαδή* $I \subseteq \mathrm{Nil}(R)$.

Απόδειξη. Εάν το $I$ είναι ένα μηδενοδύναμο ιδεώδες ενός δακτυλίου $R$, τότε $\exists n \in \mathbb{N} : I^n = \{0_R\}$, οπότε $\prod_{i=1}^{n} a_i = 0_R$ για οιαδήποτε $a_1, \ldots, a_n \in I$. Ιδιαιτέρως, για κάθε $a \in I$, $a^n = 0_R$, οπότε $a \in \mathrm{Nil}(R)$. □

**2.4.10 Σημείωση.** Εάν το $I$ είναι ιδεώδες ενός δακτυλίου $R$ με $I \subseteq \mathrm{Nil}(R)$, το $I$ δεν είναι κατ' ανάγκην μηδενοδύναμο ιδεώδες. (Για να συμβαίνει αυτό, θα πρέπει να πληρούνται κάποιες *επιπρόσθετες συνθήκες*, όπως εκείνες που περιγράφονται στην πρόταση 2.4.11.) Επί παραδείγματι, θεωρώντας τό $I := \mathrm{Nil}(R)$ (που είναι ιδεώδες βάσει τής ασκήσεως **2-6**) εντός τού μεταθετικού δακτυλίου $R := \prod_{\nu=1}^{\infty} \mathbb{Z}_{2^\nu}$ (βλ. 1.1.4 (iv) και (v)), παρατηρούμε ότι το $I$ δεν είναι μηδενοδύναμο ιδεώδες. Πράγματι· υποθέτοντας την ύπαρξη κάποιου $n \in \mathbb{N} : I^n = \{0_R\}$, θα έπρεπε να ισχύει $a^n = 0_R$ *για κάθε* στοιχείο $a \in I$, πράγμα αδύνατο, διότι π.χ. για τα στοιχεία

$$a_n := (\underbrace{[0]_{2^n}, [0]_{2^n}, \ldots, [0]_{2^n}, [0]_{2^n}}_{n \text{ φορές}}, [2]_{2^n}, [0]_{2^n}, [0]_{2^n}, \ldots) \in R$$

(τα οριζόμενα για κάθε $n \in \mathbb{N}$), έχουμε $a_n^{n+1} = 0_R$ και $a_n^n \neq 0_R$.

**2.4.11 Πρόταση.** *Εάν το $I$ είναι ένα πεπερασμένως παραγόμενο ιδεώδες ενός μεταθετικού δακτυλίου $R$ με μοναδιαίο στοιχείο και $I \subseteq \mathrm{Nil}(R)$, τότε το $I$ είναι μηδενοδύναμο ιδεώδες.*

Απόδειξη. Εάν $I = \langle a_1, \ldots, a_\kappa \rangle$, τότε (εξ υποθέσεως) $\exists n_j \in \mathbb{N} : a_j^{n_j} = 0_R$ για κάθε $j \in \{1, \ldots, \kappa\}$. Έστω $n := \max\{n_j | j \in \{1, \ldots, \kappa\}\}$ και έστω $x$ τυχόν στοιχείο τού $I$. Προφανώς,

$$a_j^n = 0_R, \ \forall j \in \{1, \ldots, \kappa\}. \tag{2.2}$$

Κατά το (iii) τής προτάσεως 2.2.2 υπάρχουν $r_1, \ldots, r_\kappa \in R$, τέτοια ώστε να ισχύει η ισότητα $x = \sum_{j=1}^{\kappa} r_j a_j$ . Επειδή ο $R$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, έχουμε (λόγω τού ορισμού τού $n$, των ισοτήτων (2.2) και τού τύπου (1.3))

$$\left( \sum_{j=1}^{\kappa} r_j a_j \right)^{\kappa n} = 0_R \Longrightarrow x^{\kappa n} = 0_R, \ \forall x \in I.$$

Σημειωτέον ότι για κάθε $m \in \mathbb{N}$ ισχύει (εξ ορισμού) η ισότητα

$$\begin{aligned} I^m &= \langle \{ a_{i_1} a_{i_2} \cdots a_{i_m} \,|\, 1 \leq i_1, i_2, \ldots, i_m \leq \kappa \} \rangle \\ &= \left\langle \left\{ a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} \,\middle|\, (\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = m \right\} \right\rangle. \end{aligned}$$

Ειδικότερα, για $m = \kappa n$ λαμβάνουμε

$$I^{\kappa n} = \left\langle \left\{ a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} \,\middle|\, (\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = \kappa n \right\} \right\rangle$$

Θα αποδείξουμε ότι $I^{\kappa n} = \{0_R\}$. Προς τούτο αρκεί να αποδείξουμε ότι όλοι οι γεννήτορες τού $I^{\kappa n}$ είναι ίσοι με το $0_R$. Όμως κάθε γεννήτοράς του (βάσει των προαναφερθέντων) είναι τής μορφής $a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa}$, όπου

$$(\lambda_1, \lambda_2, \ldots, \lambda_\kappa) \in \mathbb{N}_0^\kappa : \sum_{j=1}^{\kappa} \lambda_j = \kappa n.$$

Ως εκ τούτου, υπάρχει *τουλάχιστον ένας* δείκτης $\xi \in \{1, \ldots, \kappa\}$ με[5] $\lambda_\xi \geq n$, απ' όπου έπεται ότι

$$\begin{aligned} a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_\kappa^{\lambda_\kappa} &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} a_\xi^{\lambda_\xi} a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} \\ &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} \left( a_\xi^n a_\xi^{\lambda_\xi - n} \right) a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} \\ &= a_1^{\lambda_1} \cdots a_{\xi-1}^{\lambda_{\xi-1}} \left( 0_R \cdot a_\xi^{\lambda_\xi - n} \right) a_{\xi+1}^{\lambda_{\xi+1}} \cdots a_\kappa^{\lambda_\kappa} = 0_R. \end{aligned}$$

Άρα τελικώς $I^{\kappa n} = \{0_R\}$. □

**2.4.12 Ορισμός.** Έστω ότι ο $R$ είναι ένας μεταθετικός δακτύλιος και τα $I, J$ δυο ιδεώδη του. Το **πηλίκο** $I : J$ τού $I$ διά τού $J$ ορίζεται ως

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

και αποτελεί ένα ιδεώδες τού $R$.

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

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

[5] Αλλιώς θα είχαμε $\sum_{j=1}^{\kappa} \lambda_j < \kappa n$.

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

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

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

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

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $a \in \langle m\rangle \cap \langle n\rangle$ . Τότε $a \in \langle m\rangle$ και $a \in \langle n\rangle$, οπότε $a = \lambda m = \kappa m$, για κάποιους $\lambda, \kappa \in \mathbb{Z}$. Έστω $d := \text{μκδ}(m, n)$. Προφανώς,

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

κι επειδή $\text{μκδ}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, έχουμε $\left.\frac{n}{d}\right| \lambda \Longrightarrow \lambda = \nu\, \frac{n}{d}$, για κάποιον $\nu \in \mathbb{Z}$. Κατά συνέπειαν,

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

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

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

όπου $\frac{\mu\, \text{sgn}(m)\, |n|}{\text{μκδ}(m,n)} \in \mathbb{Z}$ και $\frac{\mu\, \text{sgn}(n)\, |m|}{\text{μκδ}(m,n)} \in \mathbb{Z}$. Συνεπώς έχουμε $a \in \langle m\rangle \cap \langle n\rangle$, δηλαδή $\langle \text{εκπ}(m,n)\rangle \subseteq \langle m\rangle \cap \langle n\rangle$ .

(ii) Κατά το (i) τής προτάσεως 2.4.3, $\langle m\rangle + \langle n\rangle = \{\, xm + yn \mid x, y \in \mathbb{Z}\}$. Επειδή ο μέγιστος κοινός διαιρέτης των $m$ και $n$ γράφεται ως ακέραιος γραμμικός συνδυασμός των $m$ και $n$, έχουμε

$$\text{μκδ}(m, n) \in (\langle m\rangle + \langle n\rangle) \Longrightarrow \langle \text{μκδ}(m, n)\rangle \subseteq \langle m\rangle + \langle n\rangle\, .$$

Και αντιστρόφως· εάν $d := \text{μκδ}(m, n)$ και $a \in \langle m\rangle + \langle n\rangle$, τότε

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

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

(iii) Προφανές επί τη βάσει τού (ii) τής προτάσεως 2.4.3.

(iv) Ας υποθέσουμε ότι $r \in \langle m\rangle : \langle n\rangle$. Τότε -εξ ορισμού- $ra \in \langle m\rangle$ για κάθε στοιχείο $a \in \langle n\rangle$. Ιδιαιτέρως, $rn \in \langle m\rangle \Rightarrow [\exists b \in \mathbb{Z} : rn = bm]$ . Εάν $d := \text{μκδ}(m, n)$, τότε $\text{μκδ}(\frac{m}{d}, \frac{n}{d}) = 1$, οπότε

$$r\, \frac{n}{d} = b\, \frac{m}{d} \Longrightarrow \left.\frac{n}{d}\right| b\frac{m}{d} \Longrightarrow \left.\frac{n}{d}\right| b \Longrightarrow b = c\frac{n}{d},$$

για κάποιον $c \in \mathbb{Z}$. Άρα

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

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

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

ήτοι $\left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle \subseteq \langle m\rangle : \langle n\rangle$. □

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

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

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

(iii) $(I_1 : I_2)\, I_2 \subseteq I_1, \quad I_1 \subseteq ((I_1\, I_2) : I_2)\,,$

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

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν στοιχείο $r \in (I_1 : I_3) + (I_2 : I_3)$. Τότε $r = r_1 + r_2$, όπου $r_1 \in (I_1 : I_3)$ και $r_2 \in (I_2 : I_3)$. Ως εκ τούτου,

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

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

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

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

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

οπότε

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

Εν συνεχεία υποθέτουμε ότι $r \in (I_1 \cap I_2) : I_3$, ήτοι ότι ισχύει η εγκλειστική σχέση $rI_3 \subseteq I_1 \cap I_2$. Επειδή $I_1 \cap I_2 \subseteq I_1$ και $I_1 \cap I_2 \subseteq I_2$, έχουμε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$,

δηλαδή $r \in (I_1 : I_3) \cap (I_2 : I_3)$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) \cap (I_2 : I_3)$, τότε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, οπότε $rI_3 \subseteq I_1 \cap I_2 \Longrightarrow r \in (I_1 \cap I_2) : I_3$.
(iii) Έστω τυχόν $r \in (I_1 : I_2)\ I_2$. Τότε

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

οπότε

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

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

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

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

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

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

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

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

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

οπότε όντως $J_1 = J_2$. □

## 2.5 ΠΡΩΤΑ ΚΑΙ ΜΕΓΙΣΤΙΚΑ ΙΔΕΩΔΗ

**2.5.1 Ορισμός.** έστω $R$ ένας δακτύλιος. Ένα ιδεώδες $\mathfrak{p}$ τού $R$ καλείται **πρώτο ιδεώδες** όταν $\mathfrak{p} \subsetneqq R$ και για οιαδήποτε ιδεώδη $I, J$ τού $R$ ισχύει η συνεπαγωγή

$$[IJ \subseteq \mathfrak{p} \Longrightarrow \text{είτε } \ I \subseteq \mathfrak{p} \ \text{ είτε } \ J \subseteq \mathfrak{p}].$$

**2.5.2 Πρόταση.** *Κάθε ιδεώδες $\mathfrak{p} \subsetneqq R$ ενός δακτυλίου $R$, για το οποίο ισχύει η συνεπαγωγή*

$$[ab \in \mathfrak{p} \Longrightarrow \text{είτε} \;\; a \in \mathfrak{p} \;\; \text{είτε} \;\; b \in \mathfrak{p}], \quad \forall\, (a,b) \in R \times R, \tag{2.3}$$

*είναι πρώτο. Και αντιστρόφως· εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες ενός δακτυλίου $R$ και ο $R$ είναι μεταθετικός, τότε το $\mathfrak{p}$ ικανοποιεί την* (2.3).

Αποδειξη. Ας υποθέσουμε εν πρώτοις ότι η συνθήκη (2.3) ικανοποιείται. Εάν τα $I, J$ είναι ιδεώδη τού $R$ με $IJ \subseteq \mathfrak{p}$ και $I \nsubseteq \mathfrak{p}$, τότε υπάρχει κάποιο στοιχείο $a \in I \smallsetminus \mathfrak{p}$. Για κάθε $b \in J$ έχουμε $ab \in IJ \subseteq \mathfrak{p}$, οπότε εξ υποθέσεως είτε $a \in \mathfrak{p}$ είτε $b \in \mathfrak{p}$. Επειδή $a \notin \mathfrak{p}$, αυτό σημαίνει ότι $b \in \mathfrak{p}$ *για κάθε* $b \in J$. Άρα $J \subseteq \mathfrak{p}$ και το $\mathfrak{p}$ είναι πρώτο ιδεώδες τού $R$. Και αντιστρόφως· εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες ενός μεταθετικού δακτυλίου $R$ και $ab \in \mathfrak{p}$, τότε το κύριο ιδεώδες $\langle ab \rangle$ περιέχεται στο $\mathfrak{p}$. Λόγω τής μεταθετικότητας τού $R$ (βλ. 2.2.4 (iii)) έχουμε

$$\left.\begin{array}{l} \langle a \rangle \langle b \rangle \subseteq \langle ab \rangle \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ πρώτο ιδεώδες} \end{array}\right\} \Longrightarrow \text{είτε} \;\; \langle a \rangle \subseteq \mathfrak{p} \;\; \text{είτε} \;\; \langle b \rangle \subseteq \mathfrak{p},$$

οπότε είτε $a \in \mathfrak{p}$ είτε $b \in \mathfrak{p}$ και το $\mathfrak{p}$ ικανοποιεί την (2.3). □

**2.5.3 Παραδείγματα.** (i) Το τετριμμένο ιδεώδες $\{0_R\}$ οιασδήποτε ακεραίας περιοχής $R$ είναι πρώτο, διότι για οιαδήποτε $a, b \in R$ ισχύει η αμφίπλευρη συνεπαγωγή

$$ab = 0_R \Longleftrightarrow \text{ είτε } a = 0_R \text{ είτε } b = 0_R.$$

(ii) Το ιδεώδες $\langle 10 \rangle$ τού δακτυλίου $\mathbb{Z}$ δεν είναι πρώτο, καθότι $2 \cdot 5 \in \langle 10 \rangle$ αλλά $2 \notin \langle 10 \rangle$ και $5 \notin \langle 10 \rangle$. Το σύνολο των πρώτων ιδεωδών τού $\mathbb{Z}$ προσδιορίζεται πλήρως στην πρόταση 2.5.4.

(iii) Το

$$I := \left\{ \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \;\middle|\; n \in \mathbb{N}_0,\ a_0 \equiv 0 (\operatorname{mod} 2) \right\}$$

είναι ένα μη κύριο ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$ (βλ. άσκηση **2-7**). Επομένως, $I \subsetneqq \mathbb{Z}[\mathsf{X}]$. Επιπροσθέτως, το $I$ είναι πρώτο ιδεώδες. Πράγματι· εάν τα

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

είναι πολυώνυμα, τέτοια ώστε $f(\mathsf{X})g(\mathsf{X}) \in I$, τότε ο σταθερός όρος $a_0 b_0$ τού $f(\mathsf{X})g(\mathsf{X})$ οφείλει να είναι άρτιος ακέραιος αριθμός. Κατ' ανάγκην λοιπόν, είτε $a_0 \equiv 0 (\operatorname{mod} 2)$ (δηλαδή $f(\mathsf{X}) \in I$) είτε $b_0 \equiv 0 (\operatorname{mod} 2)$ (δηλαδή $g(\mathsf{X}) \in I$).

(iv) Η μεταθετικότητα τού δακτυλίου $R$ είναι *αναγκαία* για να ισχύει το αντίστροφο στην πρόταση 2.5.2. Επί παραδείγματι, ο $R = \mathrm{Mat}_{n\times n}(S)$ (όπου $S$ ένας διαιρετικός δακτύλιος), $n \geq 2$, είναι μη μεταθετικός, απλός δακτύλιος (βλ. πρόταση 2.3.4), οπότε τα μόνα του ιδεώδη είναι το $\{0_R\}$ και το $R$. Ως εκ τούτου, εάν τα $I, J$ είναι ιδεώδη τού $R$ με $IJ \subseteq \{0_R\}$, έχουμε κατ' ανάγκην είτε $I = \{0_R\}$ είτε $J = \{0_R\}$. Αυτό σημαίνει ότι το τετριμμένο ιδεώδες $\{0_R\}$ είναι *πρώτο* ιδεώδες τού $R$. Ωστόσο, επειδή ο $R$ διαθέτει μηδενοδιαιρέτες, η συνθήκη (2.3) *δεν* ικανοποιείται!

**2.5.4 Πρόταση. (Πρώτα ιδεώδη τού $\mathbb{Z}$.)** *Το σύνολο των πρώτων ιδεωδών τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών απαρτίζεται από το τετριμμένο ιδεώδες και τα κύρια ιδεώδη τής μορφής $\langle p\rangle$, όπου $p$ κάποιος πρώτος αριθμός.*

Απόδειξη. Επειδή ο δακτύλιος $\mathbb{Z}$ είναι ακεραία περιοχή, το $\{0\}$ είναι πρώτο ιδεώδες του. Εάν ο $p$ είναι ένας πρώτος αριθμός και οι $a, b \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει $ab \in \langle p\rangle$, τότε

$$p \mid ab \Rightarrow \text{είτε } p \mid a \text{ είτε } p \mid b \Rightarrow \text{είτε } \; a \in \langle p\rangle \;\; \text{είτε } \; b \in \langle p\rangle\,,$$

οπότε το κύριο ιδεώδες $\langle p\rangle$ είναι πρώτο (βλ. πρόταση 2.5.2). Σύμφωνα με την πρόταση 2.2.6 κάθε μη τετριμμένο ιδεώδες τού $\mathbb{Z}$ είναι τής μορφής $\langle n\rangle$ για κάποιον $n \in \mathbb{N}$. Εάν ο $n$ είναι σύνθετος αριθμός, τότε $n = n_1 n_2$ για κάποιους φυσικούς αριθμούς $n_1, n_2$ με $1 < n_1 < n$ και $1 < n_2 < n$. Κατά συνέπειαν, $n = n_1 n_2 \in \langle n\rangle$ αλλά $n_1 \notin \langle n\rangle$ και $n_2 \notin \langle n\rangle$ (διότι κανείς εκ των $n_1, n_2$ δεν μπορεί να ισούται με κάποιο πολλαπλάσιο τού $n$). Αυτό σημαίνει ότι το ιδεώδες $\langle n\rangle$ δεν είναι πρώτο. □

**2.5.5 Παρατήρηση.** Ως γνωστόν, η τομή δυο ιδεωδών ενός δακτυλίου είναι ιδεώδες αυτού (βλ. πρόταση 2.1.5). Ωστόσο, η τομή δυο πρώτων ιδεωδών δεν είναι κατ' ανάγκην πρώτο ιδεώδες. Επί παραδείγματι, σύμφωνα με την πρόταση 2.5.4 και το (i) τού πορίσματος 2.4.13, τα ιδεώδη $\langle 3\rangle$ και $\langle 5\rangle$ είναι πρώτα ιδεώδη τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών αλλά η τομή τους $\langle 3\rangle \cap \langle 5\rangle = \langle 15\rangle$ δεν είναι πρώτο ιδεώδες. (Πρβλ. με το (i) τής ασκήσεως **2-32**.)

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

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

**2.5.7 Παραδείγματα.** (i) Το ιδεώδες $\mathfrak{m} := \{(x, 2y) \;\mid\; x, y \in \mathbb{Z}\}$ τού δακτυλίου $\mathbb{Z}\times\mathbb{Z}$ είναι μεγιστικό. Πράγματι· εάν το $\mathfrak{n}$ είναι ένα ιδεώδες τού $\mathbb{Z}\times\mathbb{Z}$, για το οποίο ισχύει

$\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq \mathbb{Z} \times \mathbb{Z}$, τότε υπάρχει κάποιο στοιχείο τής μορφής $(a, 2b+1)$ εντός τού $\mathfrak{n}$, όπου $a, b$ κατάλληλοι ακέραιοι αριθμοί. Επομένως,

$$\left.\begin{array}{r} (a, 2b+1) \in \mathfrak{n} \\ (a, 2b) \in \mathfrak{m} \subsetneqq \mathfrak{n} \end{array}\right\} \Longrightarrow (a, 2b+1) - (a, 2b) = (0, 1) \in \mathfrak{n},$$

και επειδή $(1, 0) \in \mathfrak{m}$, έχουμε $(0, 1) + (1, 0) = (1, 1) = 1_{\mathbb{Z}\times\mathbb{Z}} \in \mathfrak{n} \Longrightarrow \mathfrak{n} = \mathbb{Z} \times \mathbb{Z}$.

(ii) Το ιδεώδες

$$\mathfrak{m} = \left\{ \left( \begin{array}{cc} a & b \\ 0 & 0 \end{array} \right) \middle| \ a, b \in \mathbb{R} \right\} \subsetneqq R = \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \middle| \ c = 0 \right\}$$

τού δακτυλίου $R$ είναι μεγιστικό. Πράγματι· εάν το $\mathfrak{n}$ είναι ένα ιδεώδες τού $R$, για το οποίο ισχύει $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$, τότε υπάρχει κάποιο στοιχείο

$$\left( \begin{array}{cc} a & b \\ 0 & d \end{array} \right) \in \mathfrak{n} \smallsetminus \mathfrak{m}, \text{ με } a, b \in \mathbb{R}, \ \ d \in \mathbb{R} \smallsetminus \{0\}.$$

Επομένως,

$$\left.\begin{array}{r} \left( \begin{array}{cc} 0 & 0 \\ 0 & d^{-1} \end{array} \right) \left( \begin{array}{cc} a & b \\ 0 & d \end{array} \right) = \left( \begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \right) \in \mathfrak{n} \\ \\ \left( \begin{array}{cc} 1 & 0 \\ 0 & 0 \end{array} \right) \in \mathfrak{m} \subsetneqq \mathfrak{n} \end{array}\right\} \Longrightarrow \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \in \mathfrak{n} \Longrightarrow \mathfrak{n} = R.$$

(iii) Εντός τού δακτυλίου $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ των ακεραίων τού Gauss θεωρούμε τα ιδεώδη

$$I_p := \{a + bi \in \mathbb{Z}[i] \ : \ p \mid a \text{ και } \ p \mid b\}, \text{ όπου } p \text{ περιττός πρώτος.}$$

Το $I_3$ είναι μεγιστικό ιδεώδες τού $\mathbb{Z}[i]$. Πράγματι· εάν το $J$ είναι ένα ιδεώδες τού $\mathbb{Z}[i]$, για το οποίο ισχύει $I_3 \subsetneqq J \subseteq \mathbb{Z}[i]$, τότε υπάρχει κάποιο στοιχείο $a+bi \in J \smallsetminus I_3$ με τουλάχιστον ένα εκ των $a, b$ να μην είναι ακέραιο πολλαπλάσιο τού 3. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $3 \nmid a$ και ισχυριζόμαστε ότι $3 \nmid a^2 + b^2$. Για την απόδειξη αυτού τού ισχυρισμού θα εξετάσουμε χωριστά τις έξι δυνατές περιπτώσεις που προκύπτουν όταν κανείς εργάζεται με τις κλάσεις υπολοίπων των $a, b$ κατά μόδιο 3.

*Πρώτη περίπτωση*: Εάν $a \equiv 1 (\mathrm{mod}\, 3)$ και $b \equiv 0 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv a (\mathrm{mod}\, 3), \ b^2 \equiv 0 (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv a \equiv 1 \not\equiv 0 (\mathrm{mod}\, 3).$$

*Δεύτερη περίπτωση*: Εάν $a \equiv 1 (\mathrm{mod}\, 3)$ και $b \equiv 1 (\mathrm{mod}\, 3)$, τότε

$$\left[a^2 \equiv a (\mathrm{mod}\, 3), \ b^2 \equiv b (\mathrm{mod}\, 3)\right] \Longrightarrow a^2 + b^2 \equiv a + b \equiv 2 \not\equiv 0 (\mathrm{mod}\, 3).$$

*Τρίτη περίπτωση*: Εάν $a \equiv 1 (\bmod 3)$ και $b \equiv 2 (\bmod 3)$, τότε

$$\left[a^2 \equiv a (\bmod 3),\ b^2 \equiv 2b (\bmod 3)\right] \Longrightarrow a^2 + b^2 \equiv a + 2b \equiv 5 \equiv 2 \not\equiv 0 (\bmod 3).$$

*Τέταρτη περίπτωση*: Εάν $a \equiv 2 (\bmod 3)$ και $b \equiv 0 (\bmod 3)$, τότε

$$\left[a^2 \equiv 2a (\bmod 3),\ b^2 \equiv 0 (\bmod 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a \equiv 4 \equiv 1 \not\equiv 0 (\bmod 3).$$

*Πέμπτη περίπτωση*: Εάν $a \equiv 2 (\bmod 3)$ και $b \equiv 1 (\bmod 3)$, τότε

$$\left[a^2 \equiv 2a (\bmod 3),\ b^2 \equiv b (\bmod 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a + b \equiv 5 \equiv 2 \not\equiv 0 (\bmod 3).$$

*Έκτη περίπτωση*: Εάν $a \equiv 2 (\bmod 3)$ και $b \equiv 2 (\bmod 3)$, τότε

$$\left[a^2 \equiv 2a (\bmod 3),\ b^2 \equiv 2b (\bmod 3)\right] \Longrightarrow a^2 + b^2 \equiv 2a + 2b \equiv 8 \equiv 2 \not\equiv 0 (\bmod 3).$$

Επειδή λοιπόν $3 \nmid a^2 + b^2 \Longrightarrow$ μκδ$\left(3, a^2 + b^2\right) = 1$, υπάρχουν δύο ακέραιοι αριθμοί $k, l$, τέτοιοι ώστε να ισχύει η ισότητα $k\left(a^2 + b^2\right) + 3l = 1$. Ως εκ τούτου,

$$a + bi \in J,\ a - bi \in \mathbb{Z}[i] \Longrightarrow (a + bi)(a - bi) = a^2 + b^2 \in J$$

και

$$\left.\begin{array}{r} k \in \mathbb{Z} \subsetneqq \mathbb{Z}[i] \Rightarrow k\left(a^2 + b^2\right) \in J \\ l \in \mathbb{Z} \subsetneqq \mathbb{Z}[i] \Rightarrow 3l \in I_3 \subsetneqq J \end{array}\right\} \Longrightarrow k\left(a^2 + b^2\right) + 3l = 1 \in J,$$

απ' όπου έπεται ότι $J = \mathbb{Z}[i]$ και ότι το $I_3$ είναι ένα μεγιστικό ιδεώδες τού $\mathbb{Z}[i]$. Ωστόσο, αξιοσημείωτο είναι το ότι το $I_5$ δεν είναι μεγιστικό! Πράγματι· το κύριο ιδεώδες $I_5' = \langle 2 + i \rangle$ τού $\mathbb{Z}[i]$ περιέχει *γνησίως* το $I_5$, αφού για κάθε $a + ib \in I_5$ έχουμε

$$a + ib = (2 + i)\left(\frac{2a + b}{5} + \left(\frac{2b - a}{5}\right)i\right), \text{ όπου } \frac{2a + b}{5}, \frac{2b - a}{5} \in \mathbb{Z},$$

και $2 + i \in I_5' \smallsetminus I_5$. Θα δείξουμε ότι $I_5' \subsetneqq \mathbb{Z}[i]$ ή, ισοδυνάμως, ότι $1 \notin I_5'$. Εάν το 1 ανήκε στο $I_5'$, τότε θα έπρεπε να υπάρχουν $c, d \in \mathbb{Z}$, τέτοιοι ώστε να ισχύει η ισότητα

$$1 = (2 + i)(c + di) \Longleftrightarrow \left\{\begin{array}{c} 2c - d = 1 \\ c + 2d = 0 \end{array}\right\} \Longrightarrow c = \tfrac{2}{5},\ d = \tfrac{-1}{5},$$

από την οποία θα καταλήγαμε σε άτοπο, αφού κατ' ανάγκην $c, d \in \mathbb{Q} \smallsetminus \mathbb{Z}$.

(iv) Το κύριο ιδεώδες $\langle \mathsf{X} \rangle$ τού $\mathbb{Z}[\mathsf{X}]$ δεν είναι μεγιστικό, αφού $\langle \mathsf{X} \rangle \subsetneqq I \subsetneqq \mathbb{Z}[\mathsf{X}]$, όπου $I$ το ιδεώδες το ορισθέν στο εδάφιο 2.5.3 (iii).

**2.5.8 Πρόταση.** *Ένα γνήσιο ιδεώδες* $\mathfrak{m} \subsetneqq R$ *ενός δακτυλίου* $R$ *είναι μεγιστικό εάν και μόνον εάν*

$$\mathfrak{m} + \langle a \rangle = R, \quad \forall a \in R \smallsetminus \mathfrak{m}.$$

ΑΠΟΔΕΙΞΗ. Έστω $\mathfrak{m} \subsetneqq R$ ένα μεγιστικό ιδεώδες ενός δακτυλίου $R$. Τότε για κάθε $a \in R \smallsetminus \mathfrak{m}$ έχουμε

$$\mathfrak{m} \subsetneqq \mathfrak{m} + \langle a \rangle \subseteq R \Longrightarrow \mathfrak{m} + \langle a \rangle = R.$$

Και αντιστρόφως· εάν το $\mathfrak{m} \subsetneqq R$ είναι ένα γνήσιο ιδεώδες ενός δακτυλίου $R$ και $\mathfrak{m} + \langle a \rangle = R$ για κάθε $a \in R \smallsetminus \mathfrak{m}$, τότε για οιοδήποτε ιδεώδες $\mathfrak{n}$ τού $R$, για το οποίο ισχύουν οι εγκλεισμοί $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$, θα υπάρχει κάποιο $b \in \mathfrak{n} \smallsetminus \mathfrak{m}$. Ως εκ τούτου,

$$\left. \begin{array}{r} \mathfrak{m} \subsetneqq \mathfrak{m} + \langle b \rangle \subseteq \mathfrak{n} \\ b \in \mathfrak{n} \smallsetminus \mathfrak{m} \subseteq R \smallsetminus \mathfrak{m} \Longrightarrow \mathfrak{m} + \langle b \rangle = R \end{array} \right\} \Longrightarrow R \subseteq \mathfrak{n} \Longrightarrow \mathfrak{n} = R.$$

Άρα το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες τού $R$. $\square$

**2.5.9 Παράδειγμα.** Έστω $R = 2\mathbb{Z}$ ο δακτύλιος των αρτίων ακεραίων. Θεωρούμε το ιδεώδες $\mathfrak{m} = \langle 4 \rangle$. Σύμφωνα με το (iii) τού πορίσματος 2.2.4, αυτό το κύριο ιδεώδες μπορεί να περιγραφεί ως ακολούθως:

$$\mathfrak{m} = \langle 4 \rangle = \{ 4r + 4n \mid r \in 2\mathbb{Z},\ n \in \mathbb{Z} \} \ (= 4\mathbb{Z}).$$

Έστω $a$ τυχόν στοιχείο τού $2\mathbb{Z} \smallsetminus \mathfrak{m}$. Το $a$ οφείλει να είναι κάποιος άρτιος ακέραιος μη διαιρούμενος διά τού $4$. Κατά συνέπειαν, θα είναι τής μορφής $a = 4\lambda + 2$, για κάποιον $\lambda \in \mathbb{Z}$. Επειδή

$$2 = 4(-\lambda) + a \in \mathfrak{m} + \langle a \rangle \Longrightarrow \langle 2 \rangle \subseteq \mathfrak{m} + \langle a \rangle$$

και $\langle 2 \rangle = \{ 2r + 2n \mid r \in 2\mathbb{Z},\ n \in \mathbb{Z} \} \ (= 2\mathbb{Z})$, έχουμε $\mathfrak{m} + \langle a \rangle = 2\mathbb{Z}$, οπότε δυνάμει τής προτάσεως 2.5.8 το $\mathfrak{m} = \langle 4 \rangle$ είναι μεγιστικό ιδεώδες τού δακτυλίου $2\mathbb{Z}$.

► **Ύπαρξη μεγιστικών ιδεωδών**. Ο ορισμός 2.5.6 των μεγιστικών ιδεωδών είναι *αμιγώς συνολοθεωρητικός*. Μάλιστα, σύμφωνα με το κάτωθι θεώρημα 2.5.20, η *ύπαρξη* μεγιστικών ιδεωδών σε *δακτυλίους με μοναδιαίο στοιχείο* εξασφαλίζεται μέσω τού λεγομένου *λήμματος τού Zorn* που ισοδυναμεί με το *αξίωμα τής επιλογής*. (Προϋποθέτουμε ότι το τελευταίο συγκαταλέγεται στα λοιπά αξιώματα τής Θεωρίας Συνόλων που χρησιμοποιούμε σιωπηρώς.)

**2.5.10 Ορισμός.** Έστω $A$ ένα μη κενό σύνολο. Μια διμελής σχέση $\mathcal{R} \subseteq A \times A$ λέγεται **σχέση μερικής διατάξεως** (ή απλώς **μερική διάταξη**) επί τού $A$ όταν η $\mathcal{R}$ είναι ανακλαστική, αντισυμμετρική και μεταβατική. Σε αυτήν την περίπτωση το ζεύγος $(A, \mathcal{R})$ ονομάζεται **μερικώς διατεταγμένο σύνολο**. Συνήθως, αντί τού $\mathcal{R}$, μια σχέση μερικής διατάξεως αναπαριστάται μέσω τού συμβολισμού "$\leq$". (Επίσης χρησιμοποιείται συχνά και ο συμβολισμός «$<$» μεταξύ των στοιχείων τού $A$, όπου $x < y$ αποτελεί συντομογραφία τού ($x \leq y$ και $x \neq y$)). Ένα μερικώς διατεταγμένο σύνολο $(A, \leq)$ λέγεται **ολικώς (ή γραμμικώς) διατεταγμένο σύνολο** όταν όλα τα στοιχεία τού $A$ είναι μεταξύ τους ανά δύο *συγκρίσιμα*, δηλαδή όταν

$$(\forall x, y \in A) \;\; [x \leq y \text{ ή } y \leq x]$$

**2.5.11 Παραδείγματα.** (i) Το ζεύγος $(\mathbb{R}, \leq)$, όπου το "$\leq$" συμβολίζει τη συνήθη σχέση τού «μικρότερο ή ίσο», αποτελεί ένα ολικώς διατεταγμένο σύνολο.

(ii) Το ζεύγος $(\mathbb{Z}, <)$, όπου "$<$" η συνήθης

$$\cdots < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

ή η ακόλουθη ασυνήθης:

$$0 < -1 < 1 < -2 < 2 < -3 < 3 < \cdots$$

διάταξη των ακεραίων, αποτελεί ένα ολικώς διατεταγμένο σύνολο.

(iii) Έστω $C$ ένα σύνολο. Ορίζοντας επί τού δυναμοσυνόλου του $\mathfrak{P}(C)$ τη σχέση

$$A \leq B \underset{\text{ορσ}}{\Longleftrightarrow} A \subseteq B, \;\; \forall\, (A, B) \in \mathfrak{P}(C)^2,$$

διαπιστώνουμε ότι το $(\mathfrak{P}(C), \leq)$ είναι ένα μερικώς διατεταγμένο σύνολο. Σημειωτέον ότι το $(\mathfrak{P}(C), \leq)$ δεν είναι εν γένει ολικώς διατεταγμένο. Επί παραδείγματι, θέτοντας $C = \mathbb{N}$ και $A = \{1\}$, $B = \{2\}$, τα $A$ και $B$ *δεν* είναι μεταξύ τους συγκρίσιμα.

(iv) Όχι μόνον το δυναμοσύνολο ενός δοθέντος συνόλου, αλλά -γενικότερα- *κάθε* σύνολο με *σύνολα* ως στοιχεία του καθίσταται μερικώς διατεταγμένο ως προς τη σχέση εγκλεισμού "$\subseteq$".

**2.5.12 Ορισμός.** Έστω ότι το $(A, \leq)$ είναι ένα μερικώς διατεταγμένο σύνολο και το $B$ ένα υποσύνολο τού συνόλου $A$.

(i) Ένα στοιχείο $x \in A$ καλείται **άνω φράγμα** τού $B$ (εντός τού $A$) ως προς την "$\leq$" όταν

$$y \leq x, \;\; \forall y \in B.$$

(ii) Ένα στοιχείο $x \in A$ καλείται **κάτω φράγμα** τού $B$ (εντός τού $A$) ως προς την "$\leq$" όταν

$$x \leq y, \;\; \forall y \in B.$$

**2.5.13 Ορισμός.** Έστω $(A, \leq)$ ένα μερικώς διατεταγμένο σύνολο.

(i) Ένα στοιχείο $x \in A$ καλείται **μεγιστικό** (ή **μεγιστοτικό**) **στοιχείο** τού $A$ (ως προς την "$\leq$") όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $x \leq y$ έχουμε $x = y$. (Στην περίπτωση όπου -εντός τού $A$- υπάρχει *μόνον ένα* $x$ με αυτήν την ιδιότητα, λέμε πως το εν λόγω $x$ είναι **το μέγιστο στοιχείο** τού $A$.)

(ii) Ένα στοιχείο $x \in A$ καλείται **ελαχιστικό** (ή **ελαχιστοτικό**) **στοιχείο** τού $A$ (ως προς την "$\leq$") όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $y \leq x$ έχουμε $x = y$. (Στην περίπτωση όπου -εντός τού $A$- υπάρχει *μόνον ένα* $x$ με αυτήν την ιδιότητα, λέμε πως το εν λόγω $x$ είναι **το ελάχιστο στοιχείο** τού $A$.)

**2.5.14 Παράδειγμα.** Εάν επί τού συνόλου $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ορίσουμε τη διμελή σχέση $x \leq y \underset{\text{ορσ}}{\Longleftrightarrow} (y = kx$ για κάποιον $k \in \mathbb{Z})$, τότε το ζεύγος $(A, \leq)$ αποτελεί ένα μερικώς, αλλά όχι και ολικώς διατεταγμένο σύνολο. Ας σημειωθεί οτι τα στοιχεία $5, 6, 7, 8$ είναι μεγιστικά στοιχεία τού $A$, ενώ το $1$ είναι το ελάχιστο στοιχείο τού $A$.

**2.5.15 Ορισμός.** Ένα μερικώς διατεταγμένο σύνολο $(A, \leq)$ λέγεται **επαγωγικώς διατεταγμένο** όταν κάθε ολικώς διατεταγμένο[6] υποσύνολό του (ως προς την "$\leq$") διαθέτει ένα άνω φράγμα.

**2.5.16 Παραδείγματα.** (i) Το $(\mathbb{R}, \leq)$, όπου "$\leq$" είναι η συνήθης διάταξη των πραγματικών αριθμών, είναι επαγωγικώς διατεταγμένο.

(ii) Το $(\mathfrak{P}(A), \subseteq)$, όπου $A$ ένα μη κενό σύνολο, δεν είναι κατ' ανάγκην επαγωγικώς διατεταγμένο. Ωστόσο, κάθε υποσύνολο τού $\mathfrak{P}(A)$ τής μορφής $\{B_1, B_2, B_3, ...\}$, όπου $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$, είναι επαγωγικώς διατεταγμένο (ως προς την "$\subseteq$").

Το ακόλουθο *λήμμα τού Zorn*[7] εφαρμόζεται σε μια πληθώρα αποδείξεων θεωρημάτων σχετιζομένων με την ύπαρξη μεγιστικών στοιχείων (ως προς δεδομένες σχέσεις διατάξεως):

**2.5.17 Λήμμα τού Zorn.** *Εάν το $(A, \leq)$ είναι ένα επαγωγικώς διατεταγμένο σύνολο, τότε για οιοδήποτε $a \in A$ υπάρχει τουλάχιστον ένα μεγιστικό στοιχείο $m$ εντός τού $A$, για το οποίο ισχύει $a \leq m$.*

Στο πλαίσιο τής Θεωρίας Συνόλων αποδεικνύεται (με τη βοήθεια τής λεγομένης *υπερπεπερασμένης επαγωγής*) το εξής:

[6] Τα ολικώς διατεταγμένα υποσύνολα τού $(A, \leq)$ καλούνται ενίοτε και **αλυσίδες**.

[7] Η ύπαρξη μεγιστικού στοιχείου αποδίδεται συνήθως στον Max August Zorn (1906-1993) λόγω τής εκ μέρους του δημοσιεύσεώς της σε ένα άρθρο στο περιοδικό Bulletin of A.M.S. το 1935 (με τίτλο: *A remark on method of trasfinite algebra*). Ωστόσο, αυτό το «λήμμα» (ή ισοδύναμες παραλλαγές του) ήταν χρόνια πριν γνωστό από εργασίες των μαθηματικών R.L. Moore (1882-1974) και K. Kuratowski (1896-1980).

**2.5.18 Θεώρημα.** *Το λήμμα τού Zorn είναι ισοδύναμο τού αξιώματος τής επιλογής.*

**2.5.19 Παρατήρηση.** (i) Έστω $R$ ένας δακτύλιος και έστω

$$\mathcal{S}_R := \{\text{ιδεώδη } I \text{ τού } R \mid I \subsetneqq R\}.$$

Το $\mathcal{S}_R$ είναι μερικώς διατεταγμένο σύνολο ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 2.5.11 (iv)), οπότε ένα ιδεώδες $\mathfrak{m} \subsetneqq R$ τού $R$ είναι μεγιστικό εάν και μόνον εάν είναι *μεγιστικό στοιχείο* τού $(\mathcal{S}_R, \subseteq)$ υπό την έννοια τού ορισμού 2.5.13.

(ii) Στον ορισμό 2.5.6 υποθέσαμε ότι το $\mathfrak{m}$ είναι αμφίπλευρο ιδεώδες. Ωστόσο, κατά τον ίδιο τρόπο μπορεί κανείς να ορίσει και *αριστερά*/*δεξιά* (όχι κατ' ανάγκην αμφίπλευρα) *μεγιστικά ιδεώδη* (εάν, βεβαίως, υποθέσει ότι η απαιτούμενη συνεπαγωγή ισχύει για κάθε *αριστερό* /*δεξιό* ιδεώδες $\mathfrak{n}$ τού $R$).

**2.5.20 Θεώρημα.** *Κάθε μη τετριμμένος δακτύλιος $R$ με μοναδιαίο στοιχείο διαθέτει πάντοτε μεγιστικά ιδεώδη. Μάλιστα, ισχύει κάτι ακόμη πιο ισχυρό: Κάθε γνήσιο ιδεώδες τού $R$ περιέχεται σε κάποιο μεγιστικό ιδεώδες τού $R$.*

ΑΠΟΔΕΙΞΗ. Έστω $I \subsetneqq R$ ένα ιδεώδες τού $R$ και έστω[8]

$$\mathcal{S}_R(I) := \{\text{ιδεώδη } J \text{ τού } R \mid I \subseteq J \subsetneqq R\}.$$

Το $\mathcal{S}_R(I)$ είναι $\neq \varnothing$ (αφού $I \in \mathcal{S}_R(I)$) και μερικώς διατεταγμένο σύνολο ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 2.5.11 (iv)). Θα αποδείξουμε ότι το $(\mathcal{S}_R(I), \subseteq)$ είναι και *επαγωγικώς διατεταγμένο* (βλ. 2.5.15). Προς τούτο θεωρούμε τυχόν ολικώς διατεταγμένο υποσύνολο $A \neq \varnothing$ τού $\mathcal{S}_R(I)$ και ορίζουμε το σύνολο

$$s(A) := \bigcup \{J \in \mathcal{S}_R(I) \mid J \in A\}.$$

Προφανώς, $J \subseteq s(A)$ για κάθε $J \in A$. Θα αποδείξουμε ότι $s(A) \in \mathcal{S}_R(I)$ (ήτοι ότι το $s(A)$ είναι *ιδεώδες* τού $R$ με $I \subseteq s(A) \subsetneqq R$). Παρατηρούμε, κατ' αρχάς, ότι $I \subseteq s(A)$ (εξ ορισμού). Εξάλλου, εάν $x, y \in s(A)$, το $x$ ανήκει σε κάποιο $J_x \in A$ και το $y$ σε κάποιο $J_y \in A$. Λόγω τής ολικής διατάξεως τού $A$ ως προς τη σχέση εγκλεισμού "$\subseteq$", είτε $J_x \subseteq J_y$ είτε $J_y \subseteq J_x$. Εάν $J_x \subseteq J_y$, τότε αμφότερα τα $x, y$ ανήκουν στο $J_y$, και επειδή το $J_y$ είναι ιδεώδες τού $R$ έχουμε

$$\left.\begin{array}{r} x - y \in J_y \subseteq s(A) \\ rx, xr, ry, yr \in J_y \subseteq s(A), \forall r \in R \end{array}\right\} \Longrightarrow s(A) \text{ ιδεώδες τού } R.$$

Με τον ίδιο τρόπο αποδεικνύουμε ότι το $s(A)$ είναι ιδεώδες τού $R$ ακόμη και όταν $J_y \subseteq J_x$. Επιπροσθέτως,

$$[J \subsetneqq R, \forall J \in A] \Longrightarrow [1_R \notin J, \forall J \in A] \Longrightarrow 1_R \notin s(A) \Longrightarrow s(A) \subsetneqq R.$$

[8] Για $I = \{0_R\}$ έχουμε $\mathcal{S}_R(\{0_R\}) = \mathcal{S}_R$, όπου $\mathcal{S}_R$ το σύνολο που ορίσαμε στο 2.5.19 (i).

Συνεπώς,

$$\left.\begin{array}{r} J \subseteq s(A),\ \forall J \in A \\ s(A) \text{ ιδεώδες τού } R \\ \text{που ανήκει στο } \mathcal{S}_R(I) \end{array}\right\} \Longrightarrow \text{το } s(A) \text{ είναι } \textit{άνω φράγμα} \text{ τού } A$$

(βλ. 2.5.12 (i)). Άρα το $(\mathcal{S}_R(I), \subseteq)$ είναι όντως επαγωγικώς διατεταγμένο. Δυνάμει τού λήμματος 2.5.17 τού Zorn υπάρχει (τουλάχιστον ένα) μεγιστικό στοιχείο $\mathfrak{m}$ εντός τού $\mathcal{S}_R(I)$ με $I \subseteq \mathfrak{m}$. Το $\mathfrak{m}$ πληροί προφανώς τις επιθυμητές συνθήκες. □

**2.5.21 Παρατήρηση.** (i) Το θεώρημα 2.5.20 παραμένει εν ισχύ ακόμη και εάν κανείς αντικαταστήσει τα (αμφίπλευρα) μεγιστικά ιδεώδη (τής διατυπώσεως και τής αποδείξεώς του) με αριστερά μεγιστικά ιδεώδη (και αντιστοίχως, με δεξιά μεγιστικά ιδεώδη) χρησιμοποιώντας τα προαναφερθέντα στο εδάφιο 2.5.19 (ii).

(ii) Το θεώρημα 2.5.20 δεν μπορεί να γενικευθεί για τυχόντες *δακτυλίους χωρίς μοναδιαίο στοιχείο*. Το απλούστερο αντιπαράδειγμα είναι το εξής: Θεωρούμε την προσθετική ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών και εφοδιάζουμε το $\mathbb{Q}$ με τον *τετριμμένο πολλαπλασιασμό* "$\star$":

$$\mathbb{Q} \times \mathbb{Q} \ni (a, b) \longmapsto a \star b := 0 \in \mathbb{Q}.$$

Είναι άμεσος ο έλεγχος τού ότι η τριάδα $(\mathbb{Q}, +, \star)$ αποτελεί έναν δακτύλιο. Επιπροσθέτως, κάθε υποομάδα τής $(\mathbb{Q}, +)$ αποτελεί ένα ιδεώδες τού $(\mathbb{Q}, +, \star)$. Αρκεί λοιπόν να αποδειχθεί ότι η $(\mathbb{Q}, +)$ *στερείται μεγιστικών υποομάδων*[9] (αφού οιοδήποτε μεγιστικό ιδεώδες τού $(\mathbb{Q}, +, \star)$ θα όφειλε να είναι μεγιστική υποομάδα τής $(\mathbb{Q}, +)$). Ας υποθέσουμε ότι η $(\mathbb{Q}, +)$ διαθέτει κάποια μεγιστική υποομάδα $H \subsetneqq \mathbb{Q}$ και ότι $\frac{r}{s} \in \mathbb{Q} \smallsetminus H$, για κάποιους $r, s \in \mathbb{Z} \smallsetminus \{0\}$. Τότε

$$H \subsetneqq H + \left\langle \frac{r}{s} \right\rangle \subseteq \mathbb{Q} \Rightarrow H + \left\langle \frac{r}{s} \right\rangle = \mathbb{Q}, \tag{2.4}$$

όπου $\left\langle \frac{r}{s} \right\rangle$ η υποομάδα η παραγόμενη από το $\frac{r}{s}$. Επιπροσθέτως, $H \neq \{0\}$ (διότι π.χ. $\{0\} \subsetneqq \mathbb{Z} \subsetneqq \mathbb{Q}$). Κατά συνέπειαν, υπάρχουν $a, b \in \mathbb{Z} \smallsetminus \{0\} : \frac{a}{b} \in H$ με $b(\frac{a}{b}) = a \in H$. Επειδή $\frac{r}{s} \cdot \frac{1}{as} \in \mathbb{Q}$, η (2.4) διασφαλίζει την ύπαρξη κάποιου $h \in H$ και κάποιου $t \in \mathbb{Z}$, ούτως ώστε να ισχύει η ισότητα

$$\frac{r}{s} \cdot \frac{1}{as} = h + t\left(\frac{r}{s}\right) \Rightarrow \frac{r}{s} = (as)h + (tr)a.$$

Επειδή

$$\left.\begin{array}{r} as \in \mathbb{Z},\ h \in H \Rightarrow (as)h \in H \\ tr \in \mathbb{Z},\ a \in H \Rightarrow (tr)a \in H \end{array}\right\} \Longrightarrow (as)h + (tr)a \in H$$

καταλήγουμε στο ότι $\frac{r}{s} \in H$, ήτοι σε κάτι που αντιφάσκει προς την υπόθεσή μας.

[9] Έστω $(G, +)$ μια ομάδα. Μια υποομάδα της $H$ καλείται **μεγιστική υποομάδα** όταν δεν υφίστανται υποομάδες $K$ τής $(G, +)$ με $H \subsetneqq K \subsetneqq G$.

► **Συσχετισμός πρώτων και μεγιστικών ιδεωδών**. Στα εδάφια 2.5.22, 2.5.23 και 2.5.24 διασαφηνίζεται ο τρόπος συσχετισμού των εννοιών *πρώτο* και *μεγιστικό ιδεώδες* ενός *μεταθετικού* δακτυλίου.

**2.5.22 Θεώρημα.** *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος, για τον οποίο ισχύει $RR = R$ (όπως π.χ. στην περίπτωση κατά την οποία ο $R$ διαθέτει μοναδιαίο στοιχείο), τότε κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού $R$ είναι πρώτο.*

ΑΠΟΔΕΙΞΗ. Έστω $\mathfrak{m}$ ένα μεγιστικό ιδεώδες τού $R$. Υποθέτοντας ότι υπάρχουν $a, b \in R$, για τα οποία ισχύει $ab \in \mathfrak{m}$, όπου $a \notin \mathfrak{m}$ και $b \notin \mathfrak{m}$, έχουμε

$$\left.\begin{array}{l} \mathfrak{m} \subsetneqq \mathfrak{m} + \langle a \rangle \\ \\ \mathfrak{m} \subsetneqq \mathfrak{m} + \langle b \rangle \end{array}\right\} \Longrightarrow R = \mathfrak{m} + \langle a \rangle = \mathfrak{m} + \langle b \rangle$$

(λόγω τής «μεγιστικότητας» τού $\mathfrak{m}$). Εξάλλου, επειδή ο $R$ είναι μεταθετικός και $ab \in \mathfrak{m}$, συμπεραίνουμε ότι

$$\langle a \rangle \langle b \rangle \underset{2.2.4\,\text{(iii)}}{\subseteq} \langle ab \rangle \subseteq \mathfrak{m} \subsetneqq R$$

Όμως, επειδή $R = RR$, κατόπιν εφαρμογής τού (ii) τής προτάσεως 2.4.5 λαμβάνουμε

$$R = RR = (\mathfrak{m} + \langle a \rangle)(\mathfrak{m} + \langle b \rangle) \subseteq \mathfrak{m} + \underbrace{\langle a \rangle \langle b \rangle}_{\subseteq \langle ab \rangle \subseteq \mathfrak{m}} \subseteq \mathfrak{m},$$

ήτοι κάτι το άτοπο, καθόσον $\mathfrak{m} \subsetneqq R$. Κατά συνέπειαν, είτε $a \in \mathfrak{m}$ είτε $b \in \mathfrak{m}$, οπότε το $\mathfrak{m}$ είναι πρώτο ιδεώδες τού $R$ (βλ. πρόταση 2.5.2). $\square$

**2.5.23 Παραδείγματα.** Υπάρχουν, βεβαίως, πρώτα ιδεώδη, τα οποία δεν είναι μεγιστικά. Δύο στοιχειώδη παραδείγματα είναι τα εξής:

(i) Στον δακτύλιο $\mathbb{Z}$ των ακεραίων το τετριμμένο ιδεώδες $\{0\}$ είναι πρώτο, αλλά *δεν είναι* μεγιστικό, διότι

$$\{0\} \subsetneqq n\mathbb{Z} \subsetneqq \mathbb{Z}, \;\; \forall n \in \mathbb{Z} \smallsetminus \{0, 1\}.$$

Ωστόσο, όπως θα δούμε στην πρόταση 2.5.25, τα λοιπά πρώτα ιδεώδη τού $\mathbb{Z}$ *είναι* μεγιστικά.

(ii) Επειδή ο $\mathbb{Z}$ δεν έχει μηδενοδιαιρέτες, το ιδεώδες $I = \mathbb{Z} \times \{0\} = \{(k, 0) \mid k \in \mathbb{Z}\}$ τού $\mathbb{Z} \times \mathbb{Z}$ είναι προφανώς πρώτο. Ωστόσο, δεν είναι και μεγιστικό, διότι

$$I \subsetneqq \mathbb{Z} \times 2\mathbb{Z} \subsetneqq \mathbb{Z} \times \mathbb{Z}.$$

**2.5.24 Σημείωση.** Η συνθήκη $RR = R$ είναι *αναγκαία* για να ισχύει το θεώρημα 2.5.22. Εάν, επί παραδείγματι, θεωρήσουμε το ιδεώδες $\mathfrak{m} = \langle 4 \rangle$ τού δακτυλίου $2\mathbb{Z}$ των αρτίων ακεραίων, τότε το $\mathfrak{m}$ είναι μεγιστικό (βλ. εδάφιο 2.5.9) αλλά *δεν είναι πρώτο*, καθόσον έχουμε $2 \cdot 6 \in \mathfrak{m}$, παρότι $2 \notin \mathfrak{m}$ και $6 \notin \mathfrak{m}$.

**2.5.25 Πρόταση. (Μεγιστικά ιδεώδη τού $\mathbb{Z}$.)** *Το σύνολο των μεγιστικών ιδεωδών τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών απαρτίζεται από τα κύρια ιδεώδη τής μορφής $\langle p \rangle$, όπου $p$ κάποιος πρώτος αριθμός.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με τα προαναφερθέντα στα εδάφια 2.5.4, 2.5.22 και 2.5.23 (i), το σύνολο των μεγιστικών ιδεωδών τού δακτυλίου $\mathbb{Z}$ περιέχεται στο σύνολο των κυρίων ιδεωδών τής μορφής $\langle p \rangle$, όπου $p$ κάποιος πρώτος αριθμός. Αρκεί λοιπόν να δειχθεί ο αντίστροφος εγκλεισμός. Προς τούτο θεωρούμε το ιδεώδες $\langle p \rangle$, όπου $p$ *τυχών* πρώτος αριθμός, και υποθέτουμε ότι το $\mathfrak{n}$ είναι ένα ιδεώδες τού $\mathbb{Z}$, για το οποίο ισχύει $\langle p \rangle \subsetneqq \mathfrak{n} \subseteq \mathbb{Z}$. Κατά την πρόταση 2.2.6, $\mathfrak{n} = \langle n \rangle$, όπου $n$ κατάλληλος φυσικός αριθμός. Προφανώς,

$$p \in \mathfrak{n} = \langle n \rangle \Rightarrow \exists k \in \mathbb{N} : p = kn \Rightarrow \text{είτε } [k = p,\ n = 1] \text{ είτε } [k = 1,\ n = p].$$

Το δεύτερο ενδεχόμενο αποκλείεται, καθόσον $\langle p \rangle \subsetneqq \mathfrak{n}$. Άρα $n = 1$, απ' όπου έπεται ότι $\mathfrak{n} = \langle 1 \rangle = \mathbb{Z}$. Αυτό σημαίνει ότι το κύριο ιδεώδες $\langle p \rangle$ είναι μεγιστικό. □

## 2.6 ΠΗΛΙΚΟΔΑΚΤΥΛΙΟΙ

Έστω $(R, +, \cdot)$ ένας δακτύλιος και έστω $I$ ένα ιδεώδες του. Επειδή η προσθετική ομάδα $(R, +)$ είναι αβελιανή, το ζεύγος $(I, +)$ αποτελεί μια ορθόθετη προσθετική υποομάδα της. Επομένως υπάρχει μια καλώς ορισμένη ομάδα πηλίκων $R/I$ με πρόσθεση[10]:

$$(a + I) + (b + I) := (a + b) + I\ , \quad \text{για κάθε} \quad a, b \in R. \tag{2.5}$$

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

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

**2.6.1 Πρόταση.** *Έστω $R$ ένας δακτύλιος και έστω $I$ ένα ιδεώδες αυτού. Τότε η προσθετική ομάδα πηλίκων $R/I$ μπορεί να εφοδιασθεί με τη δομή ενός δακτυλίου όταν για κάθε $a, b \in I$ ορίσουμε τον «πολλαπλασιασμό»:*

$$(a + I)\ (b + I) := (ab) + I\ . \tag{2.6}$$

[10] $a + I := \{\, a + r \mid r \in I \}\ , \ \forall a \in R.$

ΑΠΟΔΕΙΞΗ. Η πράξη τού «πολλαπλασιασμού» (2.6) είναι καλώς ορισμένη. Πράγματι· εάν υποθέσουμε ότι $a+I=a'+I$, $b+I=b'+I$, για κάποια $a,a',b,b'\in R$, τότε $a'=a+r$ και $b'=b+s$, για κάποια $r,s\in I$. Επομένως,

$$a'b'=(a+r)(b+s)=ab+as+rb+rs\Longrightarrow a'b'-ab=as+rb+rs\in I,$$

απ' όπου συνάγουμε ότι $ab+I=a'b'+I$. Επιπροσθέτως, η εν λόγω πράξη (2.6) είναι *προσεταιριστική*, διότι

$$\begin{aligned}((a+I)\,(b+I))\,(c+I) &= ((ab)+I)\,(c+I)=(ab)\,c+I\\ &= a\,(bc)+I=(a+I)\,((bc)+I)\\ &= (a+I)\,((b+I)\,(c+I)),\end{aligned}$$

και τόσον εξ *αριστερών* όσον και εκ *δεξιών επιμεριστική* ως προς την πρόσθεση (2.5), διότι

$$\begin{aligned}(a+I)\,((b+I)+(c+I)) &= (a+I)\,((b+c)+I)\\ &= a(b+c)+I=(ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= ((a+I)\,(b+I))+((a+I)\,(c+I))\end{aligned}$$

και

$$\begin{aligned}((a+I)\,+(b+I))\,(c+I) &= ((a+b)+I)\,(c+I)\\ &= (a+b)c+I=(ac+bc)+I\\ &= ((ac)+I)+((bc)+I)\\ &= ((a+I)\,(c+I))+((b+I)\,(c+I)),\end{aligned}$$

για οιαδήποτε $a,b,c\in R$. □

**2.6.2 Ορισμός.** Ο δακτύλιος $R/I$ ονομάζεται **πηλικοδακτύλιος** (ή **δακτύλιος κλάσεων υπολοίπων**) τού $R$ ως προς το $I$.

**2.6.3 Πρόταση.** *Έστω $I$ ένα ιδεώδες ενός δακτυλίου $R$. Τότε ισχύουν τα εξής:*

(i) *Εάν ο $R$ είναι μεταθετικός, τότε και ο $R/I$ είναι μεταθετικός.*

(ii) *Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε και ο $R/I$ έχει μοναδιαίο στοιχείο, και μάλιστα $1_{R/I}=1_R+I$.*

(iii) *Εάν ο $R$ έχει μοναδιαίο στοιχείο και $a\in R^\times$, τότε $a+I\in(R/I)^\times$, και μάλιστα $(a+I)^{-1}=a^{-1}+I$.*

(iv) *Εάν $a\in R$, τότε $a+I\in\mathrm{Nil}(R/I)\Longleftrightarrow\exists n\in\mathbb{N}:a^n\in I$.*

(v) *Εάν $a\in R$, τότε το $a+I$ είναι ταυτοδύναμο στοιχείο τού πηλικοδακτυλίου $R/I\Longleftrightarrow a^2-a\in I$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν ο $R$ είναι μεταθετικός, τότε για κάθε $a, b \in R$ έχουμε

$$(a+I)(b+I) = (ab) + I = (ba) + I = (b+I)(a+I).$$

(ii) Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε για κάθε $a \in R$ έχουμε

$$(a+I)(1_R+I) = (a \cdot 1_R) + I = a + I = (1_R \cdot a) + I = (1_R + I)(a+I).$$

(iii) Εάν ο $R$ έχει μοναδιαίο στοιχείο και $a \in R^\times$, τότε $1_{R/I} = 1_R + I$ και υπάρχει το αντίστροφό $a^{-1}$ τού $a$, οπότε

$$\begin{aligned}(a+I)(a^{-1}+I) &= (a \cdot a^{-1}) + I = 1_R + I \\ &= (a^{-1} \cdot a) + I = (a^{-1}+I)(a+I).\end{aligned}$$

(iv) Εάν $a \in R$, τότε

$$\begin{gathered} a + I \in \mathbf{Nil}(R/I) \Longleftrightarrow \exists n \in \mathbb{N} : (a+I)^n = 0_{R/I} = I \\ \Longleftrightarrow \exists n \in \mathbb{N} : a^n + I = I \Longleftrightarrow \exists n \in \mathbb{N} : a^n \in I. \end{gathered}$$

(v) Έστω $a \in R$. Το $a + I$ είναι ταυτοδύναμο στοιχείο τού πηλικοδακτυλίου $R/I$ εάν και μόνον εάν

$$\begin{gathered} (a+I)^2 + ((-a)+I) = 0_{R/I} = I \Longleftrightarrow \left(a^2 + I\right) + ((-a)+I) = I \\ \Longleftrightarrow \left(a^2 - a\right) + I = I \Longleftrightarrow a^2 - a \in I, \end{gathered}$$

οπότε και αυτή η αμφίπλευρη συνεπαγωγή είναι αληθής. □

**2.6.4 Θεώρημα.** *Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και το $\mathfrak{p}$ ένα ιδεώδες τού $R$, τότε τα ακόλουθα είναι ισοδύναμα:*

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

(ii) *Ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι μεταθετικός με το $0_R + \mathfrak{p}$ ως μηδενικό και το $1_R + \mathfrak{p}$ ως μοναδιαίο του στοιχείο.

(i)⇒(ii): Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού $R$, τότε $1_R + \mathfrak{p} \neq \mathfrak{p}$ αφού $\mathfrak{p} \subsetneqq R$. Για οιαδήποτε $a, b \in R$, για τα οποία ισχύει η ισότητα $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$, έχουμε

$$ab + \mathfrak{p} = \mathfrak{p} \Rightarrow ab \in \mathfrak{p} \Longrightarrow [\text{είτε } a \in \mathfrak{p} \text{ είτε } b \in \mathfrak{p}] \Rightarrow [\text{είτε } a + \mathfrak{p} = \mathfrak{p} \text{ είτε } b + \mathfrak{p} = \mathfrak{p}].$$

Άρα ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι μια ακεραία περιοχή.

(ii)⇒(i): Εάν ο $R/\mathfrak{p}$ είναι ακεραία περιοχή, τότε $1_R + \mathfrak{p} \neq 0_R + \mathfrak{p}$, απ' όπου έπεται ότι $1_R \notin \mathfrak{p} \Longrightarrow \mathfrak{p} \subsetneqq R$. Εάν τώρα $a, b \in R$ και $ab \in \mathfrak{p}$, έχουμε

$$ab + \mathfrak{p} = \mathfrak{p} \Longrightarrow (a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}.$$

Επειδή ο πηλικοδακτύλιος $R/\mathfrak{p}$ δεν διαθέτει μηδενοδιαιρέτες, από την τελευταία αυτή ισότητα συνάγουμε ότι

$$[\text{είτε } a+\mathfrak{p}=\mathfrak{p} \text{ είτε } b+\mathfrak{p}=\mathfrak{p}] \Longrightarrow [\text{είτε } a\in\mathfrak{p} \text{ είτε } b\in\mathfrak{p}],$$

πράγμα που σημαίνει ότι το $\mathfrak{p}$ είναι πρώτο ιδεώδες τού δακτυλίου $R$ βάσει τής προτάσεως 2.5.2. □

**2.6.5 Πόρισμα.** *Έστω $\mathfrak{m}$ ένα ιδεώδες ενός μη τετριμμένου δακτυλίου $R$ με μοναδιαίο στοιχείο. Τότε ισχύουν τα ακόλουθα:*

(i) *Εάν το $\mathfrak{m}$ είναι μεγιστικό και ο $R$ μεταθετικός, τότε ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα.*

(ii) *Εάν ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι διαιρετικός δακτύλιος (=στρεβλό σώμα), τότε το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες.*

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με το θεώρημα 2.5.22, το $\mathfrak{m}$, όντας εξ υποθέσεως μεγιστικό, θα είναι και πρώτο ιδεώδες τού δακτυλίου $R$. Συνεπώς, βάσει τού θεωρήματος 2.6.4, ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι μια ακεραία περιοχή. Αρκεί λοιπόν να δείξουμε την ύπαρξη πολλαπλασιαστικού αντιστρόφου (εντός τού $R/\mathfrak{m}$) για οιοδήποτε στοιχείο $a+\mathfrak{m}\in R/\mathfrak{m}$, με $a\in R\smallsetminus\mathfrak{m}$. Επειδή το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού $R$, για οιοδήποτε μη μηδενικό στοιχείο $a+\mathfrak{m}$ τού $R/\mathfrak{m}$ έχουμε

$$\mathfrak{m}\subsetneqq\mathfrak{m}+\langle a\rangle\subseteq R \;\Longrightarrow\; \left.\begin{array}{r}\mathfrak{m}+\langle a\rangle=R\\ R\text{ μεταθετικός}\end{array}\right\}\Longrightarrow[\exists r\in R,\ b\in\mathfrak{m}:1_R=b+ra].$$

Επομένως, $1_R-ra=b\in\mathfrak{m}$, οπότε

$$1_R+\mathfrak{m}=(ra+b)+\mathfrak{m}=ra+\mathfrak{m}=(r+\mathfrak{m})\,(a+\mathfrak{m}),$$

απ' όπου έπεται ότι το $r+\mathfrak{m}$ είναι πολλαπλασιαστικό αντίστροφο τού $a+\mathfrak{m}$. Άρα ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα.

(ii) Εάν ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι διαιρετικός δακτύλιος, παρατηρούμε εν πρώτοις ότι

$$1_R+\mathfrak{m}\neq 0_R+\mathfrak{m}\Longrightarrow 1_R\notin\mathfrak{m}\Longrightarrow\mathfrak{m}\subsetneqq R.$$

Εν συνεχεία, υποθέτουμε ότι το $\mathfrak{n}$ είναι ένα ιδεώδες τού $R$ με $\mathfrak{m}\subsetneqq\mathfrak{n}\subseteq R$. Έστω τυχόν $a\in\mathfrak{n}\smallsetminus\mathfrak{m}$. Εξ υποθέσεως το $a+\mathfrak{m}$ έχει πολλαπλασιαστικό αντίστροφο, ας το πούμε $b+\mathfrak{m}$, εντός τού $R/\mathfrak{m}$. Συνεπώς,

$$(a+\mathfrak{m})\,(b+\mathfrak{m})=ab+\mathfrak{m}=1_R+\mathfrak{m}\Longrightarrow ab-1_R=:c\in\mathfrak{m}\subsetneqq\mathfrak{n},$$

και

$$\left.\begin{array}{r}a\in\mathfrak{n}\Longrightarrow ab\in\mathfrak{n}\\ c\in\mathfrak{n}\end{array}\right\}\Longrightarrow c-ab=1_R\in\mathfrak{n}\Longrightarrow\mathfrak{n}=R.$$

Άρα το $\mathfrak{m}$ είναι μεγιστικό ιδεώδες τού $R$. □

**2.6.6 Σημείωση.** Το 2.6.5 (i) δεν είναι πάντοτε αληθές για δακτυλίους χωρίς μοναδιαίο στοιχείο. Επί παραδείγματι, ο (μεταθετικός) δακτύλιος των αρτίων ακεραίων $2\mathbb{Z}$ περιέχει το μεγιστικό ιδεώδες $\mathfrak{m} = \langle 4 \rangle$ , χωρίς -όμως- ο αντίστοιχος πηλικοδακτύλιος $2\mathbb{Z}/\mathfrak{m}$ να είναι σώμα ή ακόμη και ακεραία περιοχή. Πράγματι· εντός τού πηλικοδακτυλίου υπάρχουν μηδενοδιαιρέτες, όπως π.χ. το στοιχείο $2+\mathfrak{m} \neq \mathfrak{m}$, αφού ισχύουν οι ισότητες

$$(2+\mathfrak{m})\,(2+\mathfrak{m}) = 4+\mathfrak{m} = \mathfrak{m} = 0_{2\mathbb{Z}/\mathfrak{m}}.$$

## $\boxed{2.7}$ ΤΟΠΙΚΟΙ ΔΑΚΤΥΛΙΟΙ

**2.7.1 Πρόταση.** *Έστω $R$ ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω*

$$\mathfrak{m}_{R} := R \smallsetminus R^{\times}.$$

*Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(*i*) $a - b \in \mathfrak{m}_R$ *για κάθε* $a, b \in \mathfrak{m}_R$.

(ii) *Το* $\mathfrak{m}_R$ *είναι ένα ιδεώδες τού* $R$.

(iii) *Το* $\mathfrak{m}_R$ *είναι ένα μεγιστικό ιδεώδες τού* $R$.

(iv) *Για κάθε* $a \in R$ *έχουμε είτε* $a \in R^{\times}$ *είτε* $1_R - a \in R^{\times}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Θεωρούμε τυχόντα στοιχεία $a \in \mathfrak{m}_R$ και $r \in R$. Αρκεί να αποδείξουμε ότι $ra \in \mathfrak{m}_R$. Εάν είχαμε $ra \notin \mathfrak{m}_R$, τότε $ra \in R^{\times}$, οπότε θα υπήρχε $b \in R$ με $(ra)b = a(rb) = 1_R$. Τούτο θα σήμαινε ότι $a \in R^{\times}$. Άτοπο! Άρα $ra \in \mathfrak{m}_R$.
(ii)⇒(iii): Λόγω τού (ii) τού πορίσματος 2.6.5 αρκεί προς τούτο να δειχθεί ότι ο πηλικοδακτύλιος $R/\mathfrak{m}_R$ είναι σώμα. Μάλιστα, επειδή

$$R/\mathfrak{m}_R = \left\{ r + \mathfrak{m}_R \mid r \in R^{\times} \cup \{0_R\} \right\},$$

είναι αρκετό να δειχθεί ότι $r + \mathfrak{m}_R \in (R/\mathfrak{m}_R)^{\times}$ για κάθε $r \in R^{\times}$. Τούτο έπεται από το (iii) τής προτάσεως 2.6.3.
(iii)⇒(iv): Έστω τυχόν στοιχείο $a \in R$. Εάν ίσχυε $a \in \mathfrak{m}_R$ και $1_R - a \in \mathfrak{m}_R$, τότε θα καταλήγαμε στην αντίφαση: $a + (1_R - a) = 1_R \in \mathfrak{m}_R \Longrightarrow \mathfrak{m}_R = R$.
(iv)⇒(i): Ας υποθέσουμε ότι υπάρχουν $a, b \in \mathfrak{m}_R$ με $a - b \notin \mathfrak{m}_R$. Τότε $a - b \in R^{\times}$, οπότε $\exists c \in R : (a-b)\,c = ac + (-bc) = 1_R$. Εξ υποθέσεως, είτε $ac \in R^{\times}$ είτε $-bc \in R^{\times}$. Εάν $ac \in R^{\times}$, τότε

$$\left.\begin{array}{r} a = a \cdot 1_R = (ac)\,(a-b) \\ ac \in R^{\times} \\ a - b \in R^{\times} \end{array}\right\} \Longrightarrow a \in R^{\times}.$$

Άτοπο! Αναλόγως, καταλήγουμε σε άτοπο εάν υποθέσουμε ότι $-bc \in R^{\times}$. □

**2.7.2 Ορισμός.** Κάθε μη τετριμμένος μεταθετικός δακτύλιος $R$ με μοναδιαίο στοιχείο, ο οποίος πληροί μία (και, κατ' επέκτασιν, και τις τέσσερεις) εκ των συνθηκών (i)-(iv) τής προτάσεως 2.7.1, ονομάζεται **τοπικός δακτύλιος**.

**2.7.3 Παραδείγματα.** (i) *Κάθε σώμα* $K$ *είναι ένας τοπικός δακτύλιος*, διότι το $K \diagdown K^{\times} = \{0_K\}$ είναι ιδεώδες του.

(ii) Ο δακτύλιος

$$\mathbb{Z}_{\langle p \rangle} := \left\{ r \in \mathbb{Q} \mid r = \frac{a}{b}, \ \ (a,b) \in \mathbb{Z} \times (\mathbb{Z} \diagdown \{0\}) \, , \text{ με μκδ} \, (a,b) = 1 \text{ και } p \nmid b \right\}$$

των $p$-αδικών κλασμάτων (όπου $p$ πρώτος, βλ. άσκηση **1-11**, σελ. 32) είναι τοπικός δακτύλιος, καθότι το (κύριο) ιδεώδες

$$\mathbb{Z}_{\langle p \rangle} \diagdown \mathbb{Z}_{\langle p \rangle}^{\times} = p\mathbb{Z}_{\langle p \rangle}$$

είναι μεγιστικό (οπότε πληρούται η συνθήκη (iii) τής προτάσεως 2.7.1). Πράγματι· εάν το $I$ είναι ένα ιδεώδες τού $\mathbb{Z}_{\langle p \rangle}$ με $p\mathbb{Z}_{\langle p \rangle} \subsetneqq I$, τότε

$$\exists r \in I : r \notin p\mathbb{Z}_{\langle p \rangle} \Longrightarrow r = \frac{a}{b}, \ \ (a,b) \in \mathbb{Z} \times (\mathbb{Z} \diagdown \{0\}) \, , \text{ με μκδ} \, (a,b) = 1, \ p \nmid a, \ p \nmid b.$$

Κατά συνέπειαν, $\frac{1}{r} \in \mathbb{Z}_{\langle p \rangle} \Longrightarrow \frac{1}{r} r = 1 \in I \Longrightarrow I = \mathbb{Z}_{\langle p \rangle}$.

(iii) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών δεν είναι τοπικός δακτύλιος, διότι το σύνολο $\mathbb{Z} \diagdown \mathbb{Z}^{\times} = \mathbb{Z} \diagdown \{\pm 1\}$ (εφοδιασμένο με την πράξη τής συνήθους προσθέσεως ακεραίων) δεν είναι ούτε καν υποομάδα τής ομάδας $(\mathbb{Z}, +)$, με αποτέλεσμα να μην ικανοποιείται η συνθήκη (i) τής προτάσεως 2.7.1.

(iv) Έστω $K$ ένα σώμα. Τότε ο δακτύλιος $K[\mathsf{X}]$ των πολυωνύμων μιας μεταβλητής με συντελεστές ειλημμένους από αυτό δεν είναι τοπικός δακτύλιος, διότι το σύνολο

$$K[\mathsf{X}] \diagdown K[\mathsf{X}]^{\times} = \{0_{K[\mathsf{X}]}\} \cup \{ f(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(f(\mathsf{X})) \geq 1 \}$$

(εφοδιασμένο με την πράξη τής συνήθους προσθέσεως πολυωνύμων ανηκόντων στον $K[\mathsf{X}]$) δεν είναι ούτε καν υποομάδα τής ομάδας $(K[\mathsf{X}], +)$. Αντιθέτως, ο δακτύλιος δακτύλιος $K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας μεταβλητής με συντελεστές ειλημμένους από το $K$ *είναι* τοπικός δακτύλιος. Πράγματι· ένα στοιχείο τού $K[\![\mathsf{X}]\!]$ είναι αντιστρέψιμο όταν ο σταθερός του όρος είναι $\neq 0_K$. Επομένως, το σύνολο $K[\![\mathsf{X}]\!] \diagdown K[\![\mathsf{X}]\!]^{\times}$ απαρτίζεται από εκείνες τις επίτυπες δυναμοσειρές, ο σταθερός όρος των οποίων είναι $= 0_K$ (βλ. το (iii) τής προτάσεως 1.3.9), και ισούται με

$$K[\![\mathsf{X}]\!] \diagdown K[\![\mathsf{X}]\!]^{\times} = \left\{ f(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \;\middle|\; a_0 = 0_K \right\} = \langle \mathsf{X} \rangle$$

ήτοι με το ιδεώδες το παραγόμενο από το $\mathsf{X}$. (Άρα η συνθήκη (ii) τής προτάσεως 2.7.1 ικανοποιείται και το $\langle \mathsf{X} \rangle$ είναι κατ' ανάγκην μεγιστικό ιδεώδες τού $K[\![\mathsf{X}]\!]$). Γενικότερα, ο δακτύλιος των επίτυπων δυναμοσειρών $n$ μεταβλητών $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από το $K$ *είναι* τοπικός δακτύλιος, καθότι

$$K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!] \smallsetminus K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]^{\times} = \langle \mathsf{X}_1, \ldots, \mathsf{X}_n \rangle \,.$$

**2.7.4 Πόρισμα.** *Ένας μη τετριμμένος μεταθετικός δακτύλιος $R$ με μοναδιαίο στοιχείο είναι τοπικός εάν και μόνον εάν διαθέτει ένα και μόνον μεγιστικό ιδεώδες (ήτοι το $\mathfrak{m}_R$).*

ΑΠΟΔΕΙΞΗ. Υποθέτουμε εν πρώτοις ότι ο $R$ είναι τοπικός δακτύλιος και ότι το $\mathfrak{m}$ είναι ένα μεγιστικό του ιδεώδες. Επειδή εξ ορισμού $\mathfrak{m} \subsetneqq R$, το $\mathfrak{m}$ δεν περιέχει κανένα αντιστρέψιμο στοιχείο τού $R$. Άρα $\mathfrak{m} \subseteq \mathfrak{m}_R \subsetneqq R$. Κατά τον ορισμό 2.7.2 και το (iii) τής προτάσεως 2.7.1 το $\mathfrak{m}_R$ είναι ένα μεγιστικό ιδεώδες τού $R$. Κατά συνέπειαν, $\mathfrak{m} = \mathfrak{m}_R$.

Και αντιστρόφως· εάν υποθέσουμε ότι ο $R$ είναι ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο περιέχων ένα και μόνον μεγιστικό ιδεώδες $\mathfrak{m}$ και εάν $\mathfrak{m}_R := R \smallsetminus R^{\times}$, τότε *για κάθε* $a \in \mathfrak{m}_R$ έχουμε $\langle a \rangle \subsetneqq R$ (διότι προφανώς $a \notin R^{\times} \Longrightarrow 1_R \notin \langle a \rangle$). Σύμφωνα με το θεώρημα 2.5.20 το ιδεώδες $\langle a \rangle$ οφείλει να περιέχεται σε κάποιο μεγιστικό ιδεώδες τού $R$. Όμως εξ υποθέσεως το $\mathfrak{m}$ είναι το μόνο μεγιστικό ιδεώδες τού $R$. Άρα

$$\langle a \rangle \subseteq \mathfrak{m} \subsetneqq R \Longrightarrow a \in \mathfrak{m} \Longrightarrow \mathfrak{m}_R \subseteq \mathfrak{m} \subsetneqq R.$$

Εάν υπήρχε $b \in \mathfrak{m} \smallsetminus \mathfrak{m}_R$, τότε θα είχαμε $b \in R^{\times} \cap \mathfrak{m}$, πράγμα άτοπο, καθόσον ισχύει $\mathfrak{m} \subsetneqq R \Longrightarrow R^{\times} \cap \mathfrak{m} = \varnothing$. Άρα τελικώς το $\mathfrak{m}_R = \mathfrak{m}$ είναι μεγιστικό ιδεώδες και ο $R$ τοπικός δακτύλιος. $\square$

**2.7.5 Σημείωση.** (i) Εξαιτίας τού πορίσματος 2.7.4 πολλοί συγγραφείς *ορίζουν* τους τοπικούς δακτυλίους ως «εκείνους τους μη τετριμμένους μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο που διαθέτουν ένα και μόνον μεγιστικό ιδεώδες»· είθισται, μάλιστα, η αναφορά σε κάποιον συγκεκριμένο τοπικό δακτύλιο να συνοδεύεται από την ταυτόχρονη παράθεση τού εν λόγω ιδεώδους του.

(ii) Εάν ο $R$ είναι ένας τοπικός δακτύλιος, τότε το ιδεώδες $\mathfrak{m}_R$ είναι *το μέγιστο στοιχείο* τού συνόλου $\mathcal{S}_R$ των γνησίων ιδεωδών τού $R$ ως προς τη σχέση εγκλεισμού "$\subseteq$" (βλ. 2.5.13 (i) και 2.5.19 (i)).

**2.7.6 Πρόταση.** *Η χαρακτηριστική οιουδήποτε τοπικού δακτυλίου ισούται είτε με $0$ είτε με $p^{\nu}$, όπου $p$ πρώτος αριθμός και $\nu \in \mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. Έστω $R$ τυχών τοπικός δακτύλιος με χαρ$(R) = n > 0$. Προφανώς, $n \geq 2$ (αφού ο $R$ είναι μη τετριμμένος). Ας υποθέσουμε ότι υπάρχουν πρώτοι αριθμοί $p, q$ με $p \mid n$, $q \mid n$ και $p \neq q$. Παρατηρούμε ότι

$$\begin{aligned} p \mid n &\Rightarrow \exists k \in \mathbb{N} : n = kp \\ &\Rightarrow 0 = n \cdot 1_R = k(p \cdot 1_R) \Rightarrow p \cdot 1_R \in \mathrm{Zdv}\,(R) \subsetneq R \smallsetminus R^{\times} =: \mathfrak{m}_R \end{aligned}$$

(βλ. προτάσεις 1.4.3 και 1.2.17). Κατ' αναλογίαν, αποδεικνύεται ότι $q \cdot 1_R \in \mathfrak{m}_R$. Επειδή μκδ$(p, q) = 1$, θα υπάρχουν $s, t \in \mathbb{Z} : sp + tq = 1$, οπότε

$$\left.\begin{aligned} 1_R = (sp + tq) \cdot 1_R = s(p \cdot 1_R) + t(q \cdot 1_R) \\ s \in \mathbb{Z}, p \cdot 1_R \in \mathfrak{m}_R \Rightarrow s(p \cdot 1_R) \in \mathfrak{m}_R \\ t \in \mathbb{Z}, q \cdot 1_R \in \mathfrak{m}_R \Rightarrow t(q \cdot 1_R) \in \mathfrak{m}_R \end{aligned}\right\} \Rightarrow 1_R \in \mathfrak{m}_R \Rightarrow \mathfrak{m}_R = R.$$

Άτοπο! Κατά συνέπειαν, υπάρχει *ένας και μόνον* πρώτος αριθμός $p$ που διαιρεί τον $n$, οπότε ο $n$ ισούται κατ' ανάγκην με $p^{\nu}$, όπου $\nu \in \mathbb{N}$. $\square$

## Ασκήσεις

**2-1.** Έστω $(R, +, \cdot)$ τυχών δακτύλιος και έστω $\varnothing \neq X \subseteq R$. Το σύνολο

$$\boxed{\mathrm{Ann}_R(X)_{\alpha} := \{r \in R \,|\, ra = 0_R, \forall a \in X\}}$$

καλείται **αριστερός μηδενιστής τού** $X$ **εντός τού** $R$ και το σύνολο

$$\boxed{\mathrm{Ann}_R(X)_{\delta} := \{r \in R \,|\, ar = 0_R, \forall a \in X\}}$$

**δεξιός μηδενιστής τού** $X$ **εντός τού** $R$. Όταν ο δακτύλιος είναι μεταθετικός, τότε αυτά τα δύο σύνολα ταυτίζονται. Σε αυτήν την περίπτωση, το ορισθέν σύνολο καλείται απλώς **μηδενιστής τού** $X$ **εντός τού** $R$ και συμβολίζεται ως $\mathrm{Ann}_R(X)$. Να αποδειχθούν τα ακόλουθα:

(i) Το $\mathrm{Ann}_R(X)_{\alpha}$ είναι ένα αριστερό ιδεώδες τού $R$.

(ii) Το $\mathrm{Ann}_R(X)_{\delta}$ είναι ένα δεξιό ιδεώδες τού $R$.

(iii) Εάν το $I$ είναι ένα αριστερό ιδεώδες τού $R$, τότε το $\mathrm{Ann}_R(I)_{\alpha}$ είναι ένα ιδεώδες τού $R$.

(iv) Εάν το $I$ είναι ένα δεξιό ιδεώδες τού $R$, τότε το $\mathrm{Ann}_R(I)_{\delta}$ είναι ένα ιδεώδες τού $R$.

(v) Εάν το $I$ είναι ένα ιδεώδες τού $R$, τότε αμφότερα τα $\mathrm{Ann}_R(I)_{\alpha}$ και $\mathrm{Ann}_R(I)_{\delta}$ είναι ιδεώδη τού $R$.

(vi) Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε $\mathrm{Ann}_R(R)_{\alpha} = \mathrm{Ann}_R(R)_{\delta} = \{0_R\}$.

**2-2.** Εάν το $I$ είναι ένα δεξιό και το $J$ ένα αριστερό ιδεώδες ενός δακτυλίου $R$, τέτοια ώστε $I \cap J = \{0_R\}$, να αποδειχθεί η ισότητα

$$ab = 0, \ \forall\, (a,b) \in I \times J.$$

**2-3.** Εάν τα $I, J$ είναι δυο ιδεώδη ενός δακτυλίου $R$ με $I \subseteq J$, να αποδειχθεί ότι το $I$ είναι ένα ιδεώδες τού $J$.

**2-4.** Έστω

$$R := \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; (a,b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \text{ με μκδ}\,(a,b) = 1 \text{ και } b \equiv 1 (\operatorname{mod} 2) \right\}$$

και έστω

$$I := \left\{ \frac{a}{b} \in R \;\middle|\; a \equiv 0 (\operatorname{mod} 2) \right\}.$$

Να αποδειχθεί ότι το $R$ είναι μια υποπεριοχή τού σώματος $\mathbb{Q}$ η οποία δεν είναι υπόσωμα αυτού. Κατόπιν τούτου, να αποδειχθεί ότι το $I$ είναι ένα ιδεώδες τής ακεραίας περιοχής $R$ το οποίο δεν είναι ιδεώδες τού $\mathbb{Q}$.

**2-5.** Εάν η $\{I_n\}_{n \in \mathbb{N}}$ είναι μια ακολουθία ιδεωδών ενός δακτυλίου $R$ με

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots,$$

να αποδειχθεί ότι η ένωση $I := \bigcup_{j=1}^{\infty} I_j$ αποτελεί ένα ιδεώδες τού $R$.

**2-6.** Να αποδειχθεί ότι το σύνολο $\mathrm{Nil}(R)$ των μηδενοδύναμων στοιχείων ενός μεταθετικού δακτυλίου $R$ είναι ένα ιδεώδες τού $R$. Εν συνεχεία, να δοθεί παράδειγμα μη μεταθετικού δακτυλίου $R$, εντός τού οποίου το $\mathrm{Nil}(R)$ δεν είναι ιδεώδες.

**2-7.** Να αποδειχθεί ότι το σύνολο

$$I := \left\{ \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \;\middle|\; n \in \mathbb{N}_0,\ a_0 \equiv 0 (\operatorname{mod} 2) \right\}$$

είναι ένα ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$ που δεν είναι κύριο.

**2-8.** Έστω ότι ο $m$ είναι ένας φυσικός αριθμός $\geq 5$ με $\sqrt{m} \notin \mathbb{Z}$ και ότι ο $p$ είναι ένας πρώτος αριθμός ο οποίος ικανοποιεί τις ακόλουθες συνθήκες: $p < m, \quad p \mid m+1, \quad p^2 \nmid m+1.$ Εάν

$$R := \left\{ \begin{pmatrix} a & b\sqrt{m} \\ -b\sqrt{m} & a \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

και

$$J_p := \left\{ \left( \begin{array}{cc} x & (py+x)\sqrt{m} \\ -(py+x)\sqrt{m} & x \end{array} \right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \;\middle|\; x, y \in \mathbb{Z} \right\},$$

να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο $R$ αποτελεί έναν μεταθετικό υποδακτύλιο τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ με μοναδιαίο στοιχείο $1_R = 1_{\mathrm{Mat}_{2\times 2}(\mathbb{R})}$ (ως προς τις συνήθεις πράξεις).

(ii) Ο $R$ είναι (συν τοις άλλοις) και ακεραία περιοχή.

(iii) Το σύνολο $J_p$ είναι ένα ιδεώδες τού $R$.

(iv) Το $J_p$ δεν είναι κύριο ιδεώδες.

**2-9.** Να αποδειχθούν τα ακόλουθα:

(i) Εντός τού δακτυλίου $\mathbb{Z}[\sqrt{-5}]$ ισχύουν οι ισότητες

$$\left\langle 2, 1+\sqrt{-5} \right\rangle = \left\langle 2, -1-\sqrt{-5} \right\rangle = \left\langle 2, 1-\sqrt{-5} \right\rangle.$$

(ii) Εντός τού δακτυλίου $\mathbb{Z}[\sqrt{2}]$ ισχύει η ισότητα

$$\left\langle 2+\sqrt{2} \right\rangle + \left\langle 6+\sqrt{2} \right\rangle = \left\langle \sqrt{2} \right\rangle.$$

(ii) Εντός τού δακτυλίου $\mathbb{Z}[\sqrt{2}]$ ισχύουν οι ισότητες

$$I + J = \left\langle 3, \sqrt{2} \right\rangle, \quad IJ = \left\langle \sqrt{2} \right\rangle,$$

όπου

$$I := \left\langle 3+\sqrt{2}, 3-\sqrt{2} \right\rangle, \quad J := \left\langle 2+\sqrt{2}, 2-\sqrt{2} \right\rangle.$$

**2-10.** Εάν τα $I$ και $J$ είναι δυο ιδεώδη ενός δακτυλίου $R$, να αποδειχθεί η αμφίπλευρη συνεπαγωγή

$$I + J = J \Longleftrightarrow I \subseteq J.$$

**2-11.** Έστω $R$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν $a_1, \ldots, a_k, b_1, \ldots, b_l \in R$, όπου $k, l \in \mathbb{N}$, να αποδειχθεί η αμφίπλευρη συνεπαγωγή

$$\langle a_1, \ldots, a_k \rangle \subseteq \langle b_1, \ldots, b_l \rangle \Longleftrightarrow [a_j \in \langle b_1, \ldots, b_l \rangle, \ \forall j \in \{1, \ldots, k\}].$$

**2-12.** Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος και το $a \in R$ ταυτοδύναμο (βλ. άσκηση **1-28**), να αποδειχθεί η ισότητα

$$Ra \cap Rb = Rab, \ \forall b \in R.$$

**2-13.** Έστω $R$ ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, εντός τού οποίου υπάρχουν $a, b \in R$, τέτοια ώστε να ισχύει $ab = 0_R$. Υποτιθεμένου ότι το ιδεώδες $Ra + Rb$ περιέχει μη μηδενοδιαιρέτες, να αποδειχθεί ότι $Ra \cap Rb = \{0_R\}$ και ότι το $a + b$ δεν είναι μηδενοδιαιρέτης εντός τού $R$.

**2-14.** Εάν τα $I$ και $J$ είναι δυο δεξιά (ή δυο αριστερά) ιδεώδη ενός δακτυλίου $R$, τότε δεν ισχύει κατ' ανάγκην η ισότητα $I\,J = J\,I$. Να επαληθευθεί αυτός ο ισχυρισμός μέσω τής παροχής καταλλήλου παραδείγματος.

**2-15.** Να αποδειχθεί ότι η χαρακτηριστική οιουδήποτε απλού δακτυλίου $R$ είναι είτε μηδέν είτε ένας πρώτος αριθμός.

**2-16.** Έστω $R$ τυχών δακτύλιος και έστω $n \in \mathbb{N}$. Να αποδειχθούν τα ακόλουθα:

(i) Εάν το $I$ είναι ένα αριστερό ιδεώδες τού $R$, τότε ο δακτύλιος $\mathrm{Mat}_{n\times n}(I)$ είναι ένα αριστερό ιδεώδες τού $\mathrm{Mat}_{n\times n}(R)$.

(ii) Εάν το $I$ είναι ένα δεξιό ιδεώδες τού $R$, τότε ο δακτύλιος $\mathrm{Mat}_{n\times n}(I)$ είναι ένα δεξιό ιδεώδες τού $\mathrm{Mat}_{n\times n}(R)$.

(iii) Εάν το $I$ είναι ένα ιδεώδες τού $R$, τότε ο δακτύλιος $\mathrm{Mat}_{n\times n}(I)$ είναι ένα ιδεώδες τού $\mathrm{Mat}_{n\times n}(R)$.

(iv) Οι απεικονίσεις

$$\left\{\begin{array}{c}\text{αριστερά ιδεώδη}\\ \text{τού } R\end{array}\right\} \ni I \longmapsto \Phi_{\alpha}(I) := \mathrm{Mat}_{n\times n}(I) \in \left\{\begin{array}{c}\text{αριστερά ιδεώδη}\\ \text{τού } \mathrm{Mat}_{n\times n}(R)\end{array}\right\},$$

$$\left\{\begin{array}{c}\text{δεξιά ιδεώδη}\\ \text{τού } R\end{array}\right\} \ni I \longmapsto \Phi_{\delta}(I) := \mathrm{Mat}_{n\times n}(I) \in \left\{\begin{array}{c}\text{δεξιά ιδεώδη}\\ \text{τού } \mathrm{Mat}_{n\times n}(R)\end{array}\right\}$$

και

$$\boxed{\{\text{ιδεώδη τού } R\} \ni I \longmapsto \Phi(I) := \mathrm{Mat}_{n\times n}(I) \in \{\text{ιδεώδη τού } \mathrm{Mat}_{n\times n}(R)\}}$$

είναι *ενριπτικές* και *διατηρούν τη σχέση εγκλεισμού*, δηλ. για οιαδήποτε αριστερά (και αντιστοίχως, δεξιά/αμφίπλευρα) ιδεώδη $I, I'$ τού $R$ με $I \subseteq I'$ έχουμε $\Phi_{\alpha}(I) \subseteq \Phi_{\alpha}(I')$ (και αντιστοίχως, $\Phi_{\delta}(I) \subseteq \Phi_{\delta}(I')$ / $\Phi(I) \subseteq \Phi(I')$).

(v) Οι απεικονίσεις $\Phi_{\alpha}$ και $\Phi_{\delta}$ δεν είναι κατ' ανάγκην επιρριπτικές (ακόμη και όταν ο $R$ έχει μοναδιαίο στοιχείο).

(vi) Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε η $\Phi$ είναι αμφιρριπτική απεικόνιση.

(vii) Όταν ο $R$ δεν έχει μοναδιαίο στοιχείο, η $\Phi$ δεν είναι κατ' ανάγκην επιρριπτική.

**2-17.** Έστω $R$ ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Εάν τα $I_1, I_2$ είναι δυο ιδεώδη τού $R$, να αποδειχθούν οι ακόλουθες ισότητες:

(i) $\mathrm{Mat}_{n\times n}(I_1 \cap I_2) = \mathrm{Mat}_{n\times n}(I_1) \cap \mathrm{Mat}_{n\times n}(I_2)$.

(ii) $\mathrm{Mat}_{n\times n}(I_1 + I_2) = \mathrm{Mat}_{n\times n}(I_1) + \mathrm{Mat}_{n\times n}(I_2)$.

(iii) $\mathrm{Mat}_{n\times n}(I_1 I_2) = \mathrm{Mat}_{n\times n}(I_1)\,\mathrm{Mat}_{n\times n}(I_2)$.

(Ως εκ τούτου, η αμφίρριψη $\Phi$ η ορισθείσα στην άσκηση **2-16** *διατηρεί τομές, αθροίσματα* και *γινόμενα* ιδεωδών τού $R$.)

**2-18.** Έστω $R$ τυχών δακτύλιος και έστω $n \in \mathbb{N}$, $n \geq 2$. Ένας πίνακας

$$\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$$

καλείται **άνω τριγωνικός** (και αντιστοίχως, **κάτω τριγωνικός**) όταν $a_{ij} = 0_R$ για $i > j$ (και αντιστοίχως, για $i < j$), και **αυστηρώς άνω τριγωνικός** (και αντιστοίχως, **αυστηρώς κάτω τριγωνικός**) όταν $a_{ij} = 0_R$ για $i \geq j$ (και αντιστοίχως, για $i \leq j$). Συμβολίζουμε ως $\mathrm{UT}_{n\times n}(R)$, $\mathrm{LT}_{n\times n}(R)$, $\mathrm{SUT}_{n\times n}(R)$ και $\mathrm{LUT}_{n\times n}(R)$ τα σύνολα των άνω, κάτω, αυστηρώς άνω και αυστηρώς κάτω πινάκων που ανήκουν στο $\mathrm{Mat}_{n\times n}(R)$. Να αποδειχθούν τα εξής:

(i) Τα $\mathrm{UT}_{n\times n}(R)$, $\mathrm{LT}_{n\times n}(R)$, $\mathrm{SUT}_{n\times n}(R)$ και $\mathrm{LUT}_{n\times n}(R)$ αποτελούν υποδακτυλίους τού δακτυλίου $\mathrm{Mat}_{n\times n}(R)$.

(ii) Το $\mathrm{SUT}_{n\times n}(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{UT}_{n\times n}(R)$.

(iii) Το $\mathrm{LUT}_{n\times n}(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{LT}_{n\times n}(R)$.

(iv) Κάθε πίνακας $\mathbf{A} \in \mathrm{SUT}_{n\times n}(R) \cap \mathrm{SLT}_{n\times n}(R)$ είναι μηδενοδύναμος (και μάλιστα ισχύει, ιδιαιτέρως, η ισότητα $\mathbf{A}^n = 0_{\mathrm{Mat}_{n\times n}(R)}$).

(v) Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε

$$\mathrm{UT}_{n\times n}(R)^\times = \left\{\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{UT}_{n\times n}(R) \;\middle|\; a_{ii} \in R^\times,\ \forall i \in \{1,\ldots,n\}\right\}$$

και, κατ' αναλογίαν,

$$\mathrm{LT}_{n\times n}(R)^\times = \left\{\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{LT}_{n\times n}(R) \;\middle|\; a_{ii} \in R^\times,\ \forall i \in \{1,\ldots,n\}\right\}.$$

**2-19.** Έστω $n$ ένας φυσικός αριθμός $\geq 2$. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός μεταθετικού δακτυλίου $R$, να αποδειχθεί η ισότητα

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

**2-20.** Έστω ότι τα $I, J$ είναι δυο ιδεώδη ενός δακτυλίου $R$ με μοναδιαίο στοιχείο. Εάν $I + J = R$, να αποδειχθεί ότι $I^m + J^n = R$ για οιουσδήποτε $m, n \in \mathbb{N}$.

**2-21.** Έστω $n$ ένας φυσικός αριθμός $\geq 2$. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός μεταθετικού δακτυλίου $R$ με μοναδιαίο στοιχείο και $I_i + J_i = R$ για κάθε $i \in \{1, \ldots, n\}$, όπου $J_i := \bigcap \{ I_j | \, j \in \{1, \ldots, n\} \smallsetminus \{i\} \}$, να αποδειχθούν οι ισότητες

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

**2-22.** Έστω ότι ο $R$ είναι ένας μεταθετικός δακτύλιος και τα $I_1, I_2, I_3$ τρία ιδεώδη του. Να αποδειχθούν τα ακόλουθα:

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

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

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

(iv) Εάν ο $R$ έχει μοναδιαίο στοιχείο, τότε $I_2 \subseteq I_1 \Longleftrightarrow I_1 : I_2 = R$.

**2-23.** Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος και το $I$ ένα ιδεώδες του, ορίζουμε το σύνολο

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

ως **το ριζικό τού** $I$. Εάν τα $I, J$ συμβολίζουν ιδεώδη τού $R$, να αποδειχθούν τα εξής:

(i) Το $\mathrm{Rad}(I)$ είναι ένα ιδεώδες τού $R$ και $I \subseteq \mathrm{Rad}(I)$.

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

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

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

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

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

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

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

(ix) $I = \mathrm{Rad}(I) \Longleftrightarrow \mathrm{Nil}(R/I) = \{0_{R/I}\} \; (= \{I\})$.

**2-24.** Έστω $m \in \mathbb{N}$, $m \geq 2$. Εάν $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $k \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, είναι η παράσταση τού $m$ ως γινομένου (κατάλληλων δυνάμεων) διακεκριμένων πρώτων αριθμών $p_1, \ldots, p_k$, να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Nil}(\mathbb{Z}_m) = \{[0]_m\} \Leftrightarrow \alpha_1 = \cdots = \alpha_k = 1$.

(ii) Το ριζικό τού κυρίου ιδεώδους $\langle m \rangle$ τού δακτυλίου $\mathbb{Z}$ των ακεραίων ισούται με

$$\mathrm{Rad}\,(\langle m \rangle) = \mathrm{Rad}\,(\langle -m \rangle) = \langle p_1 \cdots p_k \rangle.$$

**2-25.** Εάν το $I$ είναι ένα ιδεώδες ενός δακτυλίου $R$, να αποδειχθούν τα ακόλουθα:

(i) Ο πηλικοδακτύλιος $R/I$ είναι μεταθετικός εάν και μόνον εάν $ab - ba \in I$ για οιαδήποτε $a, b \in R$.

(ii) Ο πηλικοδακτύλιος $R/I$ έχει μοναδιαίο στοιχείο εάν και μόνον εάν υπάρχει κάποιο στοιχείο $e \in R$, τέτοιο ώστε να ισχύει

$$ae - a \in I \quad \text{και} \quad ea - a \in I, \quad \forall a \in R.$$

**2-26.** Έστω $R$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Να αποδειχθεί ότι τα ακόλουθα είναι ισοδύναμα:

(i) Ο $R$ είναι ακεραία περιοχή.

(ii) Το τετριμμένο ιδεώδες $\{0_R\}$ τού $R$ είναι πρώτο ιδεώδες.

**2-27.** Να αποδειχθεί ότι το κύριο ιδεώδες $\langle (\mathsf{X}-1)(\mathsf{X}-2) \rangle$ τού $\mathbb{Q}[\mathsf{X}]$ δεν είναι πρώτο ιδεώδες.

**2-28.** Να αποδειχθεί ότι ο πηλικοδακτύλιος $\mathbb{Z}_2[\mathsf{X}]/\left\langle \mathsf{X}^2+1 \right\rangle$ δεν είναι ακεραία περιοχή. (Ως εκ τούτου, το κύριο ιδεώδες $\left\langle \mathsf{X}^2+1 \right\rangle$ τής ακεραίας περιοχής $\mathbb{Z}_2[\mathsf{X}]$ δεν είναι πρώτο. Βλ. θεώρημα 2.6.4.)

**2-29.** Να αποδειχθεί ότι οι έννοιες *πρώτο* και *μεγιστικό* ιδεώδες οιουδήποτε *πεπερασμένου* μεταθετικού δακτυλίου με μοναδιαίο στοιχείο ταυτίζονται.

**2-30.** Έστω $R$ ένας δακτύλιος τού Boole (βλ. άσκηση **1-4**). Να αποδειχθούν τα εξής:

(i) Κάθε πεπερασμένως παραγόμενο ιδεώδες τού $R$ είναι κύριο ιδεώδες.

(ii) Έστω $I$ ένα μη τετριμμένο γνήσιο ιδεώδες τού $R$. Τότε το $I$ είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.

**2-31.** Έστω $M$ ένα μη κενό σύνολο και έστω $(\mathfrak{P}(M), \triangle, \cap)$ ο δακτύλιος Boole ο ορισθείς στην άσκηση **1-7**. Να αποδειχθούν τα εξής:

(i) Κάθε πεπερασμένως παραγόμενο ιδεώδες τού $\mathfrak{P}(M)$ είναι κύριο.

(ii) Κάθε κύριο ιδεώδες τού δακτυλίου $\mathfrak{P}(M)$ γράφεται υπό τη μορφή $\mathfrak{P}(M')$, όπου $\varnothing \neq M' \subseteq M$.

(iii) Το $\mathfrak{P}(M \setminus \{x\})$ είναι μεγιστικό ιδεώδες τού $\mathfrak{P}(M)$ για κάθε $x \in M$.

**2-32.** Έστω $R$ ένας μεταθετικός δακτύλιος. Να αποδειχθούν τα εξής:

(i) Εάν τα $\mathfrak{p}_1$ και $\mathfrak{p}_2$ είναι δυο πρώτα ιδεώδη τού $R$, τότε η τομή $\mathfrak{p}_1 \cap \mathfrak{p}_2$ είναι πρώτο ιδεώδες τού $R \Longleftrightarrow$ είτε $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ είτε $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$.

(ii) Εάν η $\{\mathfrak{p}_n\}_{n \in \mathbb{N}}$ είναι μια ακολουθία πρώτων ιδεωδών τού $R$ με

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \subseteq \mathfrak{p}_{n+1} \subseteq \cdots,$$

τότε η ένωση των μελών της $\bigcup_{j=1}^{\infty} \mathfrak{p}_j$ αποτελεί ένα πρώτο ιδεώδες τού $R$.

(iii) Εάν η $\{\mathfrak{p}_n\}_{n\in\mathbb{N}}$ είναι μια ακολουθία πρώτων ιδεωδών τού $R$ με

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n \supseteq \mathfrak{p}_{n+1} \supseteq \cdots,$$

τότε η τομή των μελών της $\bigcap_{j=1}^{\infty} \mathfrak{p}_j$ αποτελεί ένα πρώτο ιδεώδες τού $R$.

**2-33.** Έστω $R$ ένας μεταθετικός δακτύλιος και έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες αυτού. Εάν $n \in \mathbb{N}$ και εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη τού $R$, να αποδειχθούν οι ακόλουθες συνεπαγωγές:

(i) $I_1 \cdots I_n \subseteq \mathfrak{p} \Longleftrightarrow \exists j \in \{1, \ldots, n\} : I_j \subseteq \mathfrak{p}$.

(ii) $\mathfrak{p} = I_1 \cap \cdots \cap I_n \Longrightarrow \exists j \in \{1, \ldots, n\} : \mathfrak{p} = I_j$.

**2-34.** Έστω $R$ ένας μεταθετικός δακτύλιος και έστω $I$ ένα ιδεώδες αυτού. Εάν τα $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, $n \in \mathbb{N}$, είναι πρώτα ιδεώδη τού $R$, τέτοια ώστε $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, να αποδειχθεί ότι $\exists j \in \{1, \ldots, n\} : I \subseteq \mathfrak{p}_j$.

**2-35.** Έστω $R$ ένας δακτύλιος. Εάν τα $\mathfrak{m}_1, \mathfrak{m}_2$ είναι δυο μεγιστοτικά ιδεώδη τού $R$ και $\mathfrak{m}_1 \neq \mathfrak{m}_2$, να αποδειχθούν τα εξής:

(i) $\mathfrak{m}_1 + \mathfrak{m}_2 = R$.

(ii) Εάν ο $R$ είναι μεταθετικός με μοναδιαίο στοιχείο, τότε $\mathfrak{m}_1\mathfrak{m}_2 = \mathfrak{m}_1 \cap \mathfrak{m}_2$.

**2-36.** Έστω $R$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ως **πρώτο φάσμα τού** $R$ ορίζεται το σύνολο όλων των πρώτων ιδεωδών τού $R$, συμβολιζόμενο ως $\mathrm{Spec}(R)$. Για κάθε ιδεώδες $I$ τού $R$ εισάγουμε τον συμβολισμό:

$$\boxed{\mathbf{V}(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}.}$$

Να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Spec}(R) = \varnothing \Longleftrightarrow$ ο $R$ είναι τετριμμένος δακτύλιος.

(ii) Εάν τα $I, J$ είναι δυο ιδεώδη τού $R$, τότε $I \subseteq J \Longrightarrow \mathbf{V}(I) \supseteq \mathbf{V}(J)$.

(iii) $\mathbf{V}(I) = \varnothing \Longleftrightarrow I = R$.

(iv) $\mathbf{V}(\{0_R\}) = \mathrm{Spec}(R)$.

(v) Εάν $n \in \mathbb{N}$ και εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη τού $R$, τότε

$$\mathbf{V}(I_1) \cup \cdots \cup \mathbf{V}(I_n) = \mathbf{V}(I_1 \cdots I_n) = \mathbf{V}(I_1 \cap \cdots \cap I_n).$$

(vi) Εάν η $\{I_\lambda\}_{\lambda\in\Lambda}$ είναι μια οικογένεια ιδεωδών τού $R$, τότε

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

[*Σημείωση*: Είναι πρόδηλο εκ των ανωτέρω ότι το $\mathrm{Spec}(R)$ εφοδιάζεται με μία *τοπολογία* έχουσα τα μέλη τής οικογενείας $\{\mathbf{V}(I) \mid I$ ιδεώδες τού $R\}$ ως *κλειστά σύνολα*. Η εν λόγω τοπολογία καλείται **τοπολογία Zariski** επί τού $\mathrm{Spec}(R)$ και διαδραματίζει σημαντικό ρόλο στη Μεταθετική Άλγεβρα και στην Αλγεβρική Γεωμετρία.]

**2-37.** Έστω $R$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα υποσύνολο $\varnothing\neq\mathsf{S}\subseteq R$ καλείται **πολλαπλασιαστικώς κλειστό σύνολο** όταν $1_R\in\mathsf{S}$ και $ab\in\mathsf{S}$ για οιαδήποτε $a,b\in\mathsf{S}$. Να αποδειχθούν τα ακόλουθα:

(i) Εάν το $\mathsf{S}\subseteq R$ είναι ένα πολλαπλασιαστικώς κλειστό σύνολο και το $I$ ένα ιδεώδες τού $R$ με $I\cap\mathsf{S}=\varnothing$, τότε

$$\exists\mathfrak{p}\in\mathrm{Spec}(R):\mathfrak{p}\supseteq I\ \text{ και }\ \mathfrak{p}\cap\mathsf{S}=\varnothing.$$

[*Υπόδειξη*: Να επαληθευθεί ότι το

$$(\{J\mid J \text{ ιδεώδες τού } R \text{ με } J\supseteq I\ \text{ και } J\cap\mathsf{S}=\varnothing\},\subseteq)$$

είναι επαγωγικώς διατεταγμένο και να εφαρμοσθεί το λήμμα 2.5.17 τού Zorn.]

(ii) Για κάθε ιδεώδες $I$ τού $R$ ισχύει η ισότητα

$$\mathrm{Rad}\,(I)=\bigcap\{\mathfrak{p}\mid\mathfrak{p}\in\mathbf{V}(I)\}.$$

Σημειωτέον ότι για $I=\{0_R\}$,

$$\mathrm{Nil}\,(R)=\mathrm{Rad}\,(\{0_R\})=\bigcap\{\mathfrak{p}\mid\mathfrak{p}\in\mathrm{Spec}(R)\}.$$

[*Υπόδειξη*: Για την απόδειξη τού αντίστροφου εγκλεισμού "$\supseteq$" να υποτεθεί ότι υπάρχει στοιχείο $a\in\bigcap\{\mathfrak{p}\mid\mathfrak{p}\in\mathbf{V}(I)\}$ με $a\notin\mathrm{Rad}(I)$ και να εφαρμοσθεί το (i) για το πολλαπλασιαστικώς κλειστό σύνολο $\mathsf{S}:=\{a^n\mid n\in\mathbb{N}_0\}$, ούτως ώστε να προκύψει αντίφαση.]

**2-38.** Έστω $R$ ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν τα $I,J$ είναι ιδεώδη τού $R$, να αποδειχθούν τα ακόλουθα:

(i) $\mathbf{V}(I)\subseteq\mathbf{V}(J)\Longleftrightarrow\mathrm{Rad}(J)\supseteq\mathrm{Rad}(I)$.

(ii) $\mathbf{V}(I)=\mathbf{V}(J)\Longleftrightarrow\mathrm{Rad}(I)=\mathrm{Rad}(J)$.

(iii) $\mathbf{V}(I)=\mathrm{Spec}(R)\Longleftrightarrow I\subseteq\mathrm{Nil}(R)$.

**2-39.** Να αποδειχθεί ότι τα μόνα ταυτοδύναμα στοιχεία ενός τοπικού δακτυλίου $R$ είναι τα $0_R$ και $1_R$.

**2-40.** Έστω $m \in \mathbb{N}$, $m \geq 2$. Να αποδειχθεί ότι ο δακτύλιος $\mathbb{Z}_m$ (ο ορισθείς στο εδάφιο 1.1.4 (iv)) είναι τοπικός εάν και μόνον εάν $m = p^\nu$, όπου $p$ κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$.