ΚΕΦΑΛΑΙΟ 1

Δακτύλιοι, ακέραιες περιοχές και σώματα

Η αλγεβρική δομή ενός *δακτυλίου* [1] καθορίζεται μέσω τού εφοδιασμού ενός μη κενού συνόλου *με δύο εσωτερικές πράξεις*. Ως προς την πρώτη εξ αυτών το θεωρούμενο σύνολο οφείλει να σχηματίζει μια *αβελιανή ομάδα*· ως προς τη δεύτερη, μια *ημιομάδα*. Επιπροσθέτως, απαιτείται και η ισχύς των *επιμεριστικών νόμων* για τον συσχετισμό των εν λόγω πράξεων. Οι *ακέραιες περιοχές* είναι εκείνοι οι μη τετριμμένοι μεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο οι οποίοι δεν διαθέτουν μηδενοδιαιρέτες. Τα *σώματα* [2], από την άλλη μεριά, συγκροτούν μια ειδική υποκλάση τής κλάσεως των δακτυλίων· πρόκειται, για να ακριβολογούμε, για την υποκλάση εκείνων των *διαιρετικών δακτυλίων*, οι οποίοι συμβαίνει να είναι -ταυτοχρόνως- και μεταθετικοί.

1.1 ΔΑΚΤΥΛΙΟΙ ΚΑΙ ΥΠΟΔΑΚΤΥΛΙΟΙ

1.1.1 Ορισμός. Ένας **δακτύλιος** $(R, +, \cdot)$ είναι ένα μη κενό σύνολο R εφοδιασμένο με δύο εσωτερικές πράξεις "$+$" και "$\cdot$", που καλούνται (και συμβολίζονται ως) *πρόσθεση* και *πολλαπλασιασμός*, αντιστοίχως, ούτως ώστε

(i) το ζεύγος $(R, +)$ να είναι μια αβελιανή ομάδα,

(ii) το ζεύγος $(R, \cdot)$ να είναι μια ημιομάδα, και

[1] Η έννοια τού *δακτυλίου* εισήχθη από τον David Hilbert (1862-1943) στο τέλος τού δεκάτου ενάτου αιώνα, αλλά ο τελικώς καθιερωθείς (φορμαλιστικός) ορισμός της εμφανίσθηκε περί τα μέσα τής δεκαετίας τού 1920.

[2] Η εισαγωγή τού όρου *σώμα* (γερμ. Körper) οφείλεται στους Leopold Kronecker (1823-1891) και Richard Dedekind (1831-1916), αν και η τελική εννοιολόγησή του (που επεκράτησε έκτοτε) αποδίδεται στον Heinrich Weber (1842-1913).

(iii) η "$\cdot$" να είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "$+$", δηλαδή για κάθε a, b και $c \in R$ να ισχύει

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c\,.$$

Το ουδέτερο στοιχείο τής ομάδας $(R, +)$ καλείται **μηδενικό στοιχείο** τού R και σημειώνεται με το 0_R. Εάν η ημιομάδα $(R, \cdot)$ διαθέτει *μοναδιαίο (= πολλαπλασιαστικώς ουδέτερο) στοιχείο* (σημειούμενο ως 1_R), δηλαδή εάν η $(R, \cdot)$ είναι ένα μονοειδές, τότε και ο R καλείται **δακτύλιος με μοναδιαίο στοιχείο** (ή **1-δακτύλιος**).

1.1.2 Σημείωση. Για λόγους συντομίας, πολλές φορές αντί τού $a \cdot b$ θα γράφουμε ab, ενώ όταν θα ομιλούμε για κάποιον «δακτύλιο R», θα υπονοούμε τη θεώρηση μιας τριάδας $(R, +, \cdot)$ όπως στον ορισμό 1.1.1 χωρίς όμως και να τη σημειώνουμε. Επίσης, εάν[3] $n \in \mathbb{N}$ και εάν τα $a_1, \ldots, a_n$ είναι στοιχεία ενός δακτυλίου R, τότε χρησιμοποιούμε ενίοτε τις βραχυγραφίες

$$\sum_{i=1}^{n} a_i := a_1 + \cdots + a_n, \qquad \prod_{i=1}^{n} a_i := a_1 \cdot \cdots \cdot a_n.$$

1.1.3 Ορισμός. Ένας δακτύλιος R λέγεται **μεταθετικός** όταν η πράξη τού πολλαπλασιασμού του είναι μεταθετική, δηλαδή όταν $ab = ba$ για κάθε $a, b \in R$.

1.1.4 Παραδείγματα. (i) Τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ των ακεραίων, των ρητών, των πραγματικών και των μιγαδικών αριθμών, αντιστοίχως, εφοδιασμένα με τις συνήθεις πράξεις τής προσθέσεως και τού πολλαπλασιασμού, αποτελούν τα πιο απλά παραδείγματα μεταθετικών δακτυλίων με μοναδιαίο στοιχείο.

(ii) Έστω $(R, +, \cdot)$ τυχών δακτύλιος. Εάν τα I, J είναι δυο μη κενά πεπερασμένα υποσύνολα τού $\mathbb{N}$, τότε κάθε απεικόνιση

$$f : I \times J \longrightarrow R \tag{1.1}$$

ονομάζεται $(\mathrm{card}(I) \times \mathrm{card}(J))$-**πίνακας** (ή **μητρείο**) με τις «εγγραφές[4]» του ειλημμένες από τον R. Αντί τού (1.1) είθισται να γράφουμε

$$(a_{ij})_{(i,j)\in I\times J}, \text{ όπου } a_{ij} := f\,(i, j)\,, \text{ για κάθε } (i, j) \in I \times J.$$

Ο ορισμός αυτός εφαρμόζεται ως επί το πλείστον στην ειδική περίπτωση όπου

$$I = \{1, \ldots, m\} \text{ και } J = \{1, \ldots, n\},$$

για κάποιους $m, n \in \mathbb{N}$. Κάθε απεικόνιση

$$f : \{1, \ldots, m\} \times \{1, \ldots, n\} \longrightarrow R \tag{1.2}$$

[3] Ως συνήθως, συμβολίζουμε ως $\mathbb{N}$, $\mathbb{N}_0$ τα σύνολα των φυσικών και των μη αρνητικών ακεραίων αριθμών, αντιστοίχως.

[4] Οι **εγγραφές** (αγγλ. entries) ενός πίνακα (1.1) είναι τα στοιχεία τής εικόνας του.

είναι ένας $(m \times n)$-**πίνακας** (ή $(m \times n)$-**μητρείο**) με τις εγγραφές του ειλημμένες από τον R. Και εδώ, αντί τού σχετικώς δύσχρηστου συμβολισμού (1.2) γράφουμε απλώς

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\,n-1} & a_{1\,n} \\ a_{21} & a_{22} & \cdots & a_{2\,n-1} & a_{2\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m-1\,1} & a_{m-1\,2} & \cdots & a_{m-1\,n-1} & a_{m-1\,n} \\ a_{m\,1} & a_{m\,2} & \cdots & a_{m\,n-1} & a_{m\,n} \end{pmatrix}$$

ή $(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$, όπου

$$a_{ij} := a_{i,j} := f(i,j),\ \forall\,(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}.$$

Το σύνολο όλων των $(m \times n)$-πινάκων (με τις εγγραφές τους ειλημμένες από το R) θα συμβολίζεται ως $\mathrm{Mat}_{m\times n}(R)$. Για οιουσδήποτε πίνακες

$$\mathbf{A} = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathrm{Mat}_{m\times n}(R),\ \ \mathbf{B} = (b_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathrm{Mat}_{m\times n}(R) \tag{1.3}$$

ισχύει (προφανώς) η αμφίπλευρη συνεπαγωγή

$$\mathbf{A} = \mathbf{B} \Longleftrightarrow a_{ij} = b_{ij},\ \forall\,(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}.$$

Κάθε πίνακας $\mathbf{A} = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathrm{Mat}_{m\times n}(R)$ διαθέτει m **γραμμές**

$$\Gamma\varrho_i(\mathbf{A}) := (a_{i1}\ a_{i2}\ \cdots\ a_{i\,n-1}\ a_{i\,n}) \in \mathrm{Mat}_{1\times n}(R),\ \ i \in \{1,\dots,m\},$$

και n **στήλες**

$$\Sigma\tau_j(\mathbf{A}) := \begin{pmatrix} a_{1j} \\ \vdots \\ a_{m\,j} \end{pmatrix} \in \mathrm{Mat}_{m\times 1}(R),\ \ j \in \{1,\dots,n\}.$$

(Η $\Gamma\varrho_i(\mathbf{A})$ καλείται i-**οστή γραμμή** και η $\Sigma\tau_j(\mathbf{A})$ j-**οστή στήλη τού** $\mathbf{A}$.) Προφανώς,

$$\mathbf{A} = (\Sigma\tau_1(\mathbf{A})\ \cdots\ \Sigma\tau_n(\mathbf{A})) = \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_m(\mathbf{A}) \end{pmatrix}.$$

Εάν $r \in R$, τότε για οιονδήποτε $\mathbf{A} = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathrm{Mat}_{m\times n}(R)$ θέτουμε

$$r\mathbf{A} := (ra_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}.$$

Το $\mathrm{Mat}_{m\times n}(R)$ καθίσταται αβελιανή ομάδα με μέσω τής προσθετικής πράξεως[5]

$$\mathbf{A} + \mathbf{B} := (a_{ij} + b_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$$

[5] Το ουδέτερο στοιχείο $0_{\mathrm{Mat}_{m\times n}(R)}$ αυτής τής ομάδας είναι ο $(m \times n)$-πίνακας, όλες οι εγγραφές τού οποίου είναι ίσες με το 0_R (και είθισται να σημειώνεται εν συντομία ως $\mathbf{0}_{m\times n}$).

για οιουσδήποτε πίνακες (1.3). Στην ειδική περίπτωση όπου $m = n$, το σύνολο $\mathrm{Mat}_{n\times n}(R)$ (ήτοι το σύνολο των **τετραγωνικών πινάκων**) καθίσταται δακτύλιος μέσω αυτής τής προσθετικής πράξεως και τής πολλαπλασιαστικής πράξεως

$$\mathbf{AB} := \left(\sum_{k=1}^{n} a_{i\,k} b_{k\,j}\right)_{1\le i,j\le n},$$

για οιουσδήποτε $\mathbf{A} = (a_{ij})_{1\le i,j\le n}$ και $\mathbf{B} = (b_{ij})_{1\le i,j\le n} \in \mathrm{Mat}_{n\times n}(R)$. Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο $\mathrm{Mat}_{n\times n}(R)$ έχει μοναδιαίο στοιχείο, ήτοι τον *μοναδιαίο* $(n\times n)$*-πίνακα*

$$\mathbf{I}_n = \begin{pmatrix} 1_R & 0_R & \cdots & 0_R & 0_R \\ 0_R & 1_R & \cdots & 0_R & 0_R \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0_R & 0_R & \cdots & 1_R & 0_R \\ 0_R & 0_R & \cdots & 0_R & 1_R \end{pmatrix}.$$

Σημειωτέον ότι ο δακτύλιος $\mathrm{Mat}_{n\times n}(R)$ δεν είναι κατ' ανάγκην μεταθετικός, ακόμη και όταν ο ίδιος ο R είναι· εάν π.χ. ο R μεταθετικός με μοναδιαίο στοιχείο $1_R \neq 0_R$, τότε ο $\mathrm{Mat}_{n\times n}(R)$ δεν είναι μεταθετικός στην περίπτωση κατά την οποία $n > 1$, αφού

$$\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix}\begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix} = \begin{pmatrix} 0_R & 1_R \\ 1_R & 1_R \end{pmatrix} \neq \begin{pmatrix} 1_R & 1_R \\ 1_R & 0_R \end{pmatrix} = \begin{pmatrix} 1_R & 1_R \\ 0_R & 1_R \end{pmatrix}\begin{pmatrix} 0_R & 1_R \\ 1_R & 0_R \end{pmatrix}.$$

(Οι έννοιες: *υποπίνακας πίνακα*, *τεμαχισμένοι πίνακες*, *ελάσσονες πίνακες* κλπ. ορίζονται όπως και στη συνήθη Γραμμική Άλγεβρα. Για την εμπέδωση των απαραίτητων ιδιοτήτων των *οριζουσών πινάκων* που ανήκουν στον $\mathrm{Mat}_{n\times n}(R)$, όπου R κάποιος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_R \neq 0_R$, παροτρύνουμε τον αναγνώστη, στο σημείο αυτό, να επιλύσει την άσκηση **1-19**).

(iii) Το σύνολο $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ των άρτιων ακεραίων αριθμών με τις συνήθεις πράξεις είναι ένας μεταθετικός δακτύλιος *χωρίς* μοναδιαίο στοιχείο.

(iv) Έστω m ένας φυσικός αριθμός ≥ 1. Η διμελής σχέση ισοτιμίας

$$a \sim_m b \underset{\text{ορσ}}{\Longleftrightarrow} [\text{ο } m \text{ διαιρεί τη διαφορά } a-b]$$

αποτελεί μια σχέση ισοδυναμίας επί τού συνόλου $\mathbb{Z}$ των ακεραίων. Για να δώσουμε έμφαση στην εξάρτηση από το m συμβολίζουμε ως

$$\ldots, [-2]_m, [-1]_m, [0]_m, [1]_m, [2]_m, \ldots$$

τις κλάσεις ισοδυναμίας των ακεραίων αριθμών (ως προς την " $\sim_m$ ") και ως $\mathbb{Z}_m := \mathbb{Z}/\sim_m$το *σύνολο των κλάσεων υπολοίπων (ή κλάσεων ισοτιμίας) των ακεραίων κατά μόδιο* m (ή *modulo* m). Το $\mathbb{Z}_m$ γράφεται σε «ανηγμένη[6] μορφή» ως

[6]Τούτο σημαίνει ότι τα εντός των αγκίστρων αναγραφόμενα στοιχεία είναι *σαφώς διακεκριμένα* (ήτοι ανά δύο διαφορετικά, αποκλείοντας την επανάληψη κάποιου εξ αυτών).

ακολούθως[7]:

$$\boxed{\mathbb{Z}_m := \{[0]_m, [1]_m, \dots, [m-1]_m\}}$$

και αποτελεί έναν μεταθετικό δακτύλιο (με το $[1]_m$ ως μοναδιαίο στοιχείο[8]) βάσει των συνήθων πράξεων

$$[a]_m + [b]_m := [a+b]_m \quad \text{και} \quad [a]_m \cdot [b]_m := [ab]_m$$

για κάθε ζεύγος $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

(v) Έστω X ένα μη κενό σύνολο και έστω R ένας δακτύλιος. Τότε το σύνολο των απεικονίσεων $R^X := \{\text{απεικονίσεις } f : X \longrightarrow R\}$ καθίσταται δακτύλιος μέσω των «σημειακών» πράξεων

$$\begin{aligned} f + g : X &\longrightarrow R, \quad x \longmapsto f(x) + g(x) \\ f \cdot g : X &\longrightarrow R, \quad x \longmapsto f(x) \cdot g(x) \end{aligned}$$

Ιδιαιτέρως, εάν $X = \{1, \dots, n\} \subset \mathbb{N}$, τότε μπορούμε να ταυτίζουμε το R^X με το *καρτεσιανό γινόμενο* $\underbrace{R \times R \times \cdots \times R \times R}_{n \text{ φορές}}$, το οποίο αποκτά τη δομή τού δακτυλίου μέσω των πράξεων

$$\begin{aligned} &(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n), \\ &(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) := (x_1 \cdot y_1, x_2 \cdot y_2, \dots, x_n \cdot y_n), \end{aligned}$$

με ουδέτερο στοιχείο ως προς την πρόσθεση το $(0_R, \dots, 0_R)$. Εξάλλου, δοθέντων n αυθαιρέτως επιλεγμένων δακτυλίων $R_1, R_2, \dots, R_n$ μπορούμε να ορίσουμε τη δομή ενός δακτυλίου επί τού *καρτεσιανού* ή (*εξωτερικού*) *ευθέος γινομένου* τους

$$\prod_{j=1}^{n} R_j := R_1 \times \cdots \times R_n \tag{1.4}$$

με τις ανάλογες πράξεις κατά παράγοντες. Ο δακτύλιος (1.4) είναι μεταθετικός εάν και μόνον εάν καθένας των παραγόντων του είναι μεταθετικός. Επιπροσθέτως, ο (1.4) έχει μοναδιαίο στοιχείο εάν και μόνον εάν καθένας των παραγόντων του έχει μοναδιαίο στοιχείο. (Μάλιστα, όταν ο (1.4) έχει μοναδιαίο στοιχείο, τότε αυτό είναι το $(1_{R_1}, \dots, 1_{R_n})$.) Κατ' αναλογίαν, εάν η $(R_j)_{j \in J}$ είναι μια μη κενή οικογένεια δακτυλίων, μπορούμε να ορίσουμε τη δομή δακτυλίου επί τού $\prod\limits_{j \in J} R_j$ μέσω των πράξεων

$$(x_j)_{j \in J} + (y_j)_{j \in J} := (x_j + y_j)_{j \in J}, \ (x_j)_{j \in J} \cdot (y_j)_{j \in J} := (x_j \cdot y_j)_{j \in J}.$$

[7] Επειδή *κάθε* $a \in \mathbb{Z}$ μπορεί να γραφεί υπό τη μορφή $a = qm + r$, όπου τα q και r είναι κατάλληλοι ακέραιοι αριθμοί και $0 \leq r < m$ (ήτοι το r είναι το υπόλοιπο τής διαιρέσεως τού a διά τού m), λαμβάνουμε την ισότητα $[a]_m = [r]_m$. Εξ αυτού συνάγεται ότι οι *σαφώς διακεκριμένες* κλάσεις ισοδυναμίας που διαθέτουμε είναι οι μόνον οι $[0]_m, [1]_m, \dots, [m-1]_m$.

[8] Όταν $m = 1$, έχουμε $[0]_1 = [1]_1$.

(vi) Εάν το R είναι ένα μονοσύνολο, τότε μπορεί να θεωρηθεί κατά τρόπο τετριμμένο ως δακτύλιος και γι' αυτό ονομάζεται **τετριμμένος δακτύλιος**. Σε αυτήν την περίπτωση έχουμε προφανώς $0_R = 1_R$.

(vii) Εκκινώντας από τον $(\mathbb{Z}, +, \cdot)$ μπορούμε να κατασκευάσουμε έναν άλλο μεταθετικό δακτύλιο με μοναδιαίο στοιχείο $(\mathbb{Z}, \boxplus, \boxdot)$ μέσω των πράξεων

$$a \boxplus b := a + b - 1, \qquad a \boxdot b := a + b - ab\,.$$

Το αξιοπερίεργο εδώ είναι ότι το ουδέτερο στοιχείο αυτού τού δακτυλίου ως προς την πρόσθεση $\boxplus$ είναι το 1, ενώ το μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό $\boxdot$ είναι το 0.

(viii) Τέλος, θα άξιζε να αναφερθεί ότι υπάρχουν και μη μεταθετικοί δακτύλιοι, οι οποίοι δεν διαθέτουν μοναδιαίο στοιχείο. Επί παραδείγματι, ο

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{Z})$$

(ως προς τις συνήθεις πράξεις των 2×2 πινάκων) ή ακόμη και ο ίδιος ο $\mathrm{Mat}_{2\times 2}(2\mathbb{Z})$ είναι δακτύλιοι αυτού τού είδους.

1.1.5 Πρόταση. *Έστω R ένας δακτύλιος. Τότε ισχύουν τα εξής*:

(i) $0_R\, a = a\, 0_R = 0_R$, *για όλα τα* $a \in R$.

(ii) $(-a)\, b = a\, (-b) = -(a\, b)$, *για όλα τα* $a, b \in R$.

(iii) $(-a)\, (-b) = a\, b$, *για όλα τα* $a, b \in R$.

(iv) *Για* $m, n \in \mathbb{N}$ *και για οιαδήποτε στοιχεία* $a_1, \ldots, a_m, b_1, \ldots, b_n$ *τού* R *έχουμε*

$$\left(\sum_{j=1}^{m} a_j \right) \left(\sum_{k=1}^{n} b_k \right) = \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k \;\; .$$

(v) *Εάν για οιαδήποτε* $a \in R$ *και* $n \in \mathbb{Z}$ *χρησιμοποιήσουμε τη βραχυγραφία*

$$na := \begin{cases} \underbrace{a + a + \cdots + a + a}_{n\text{-φορές}}, & \text{όταν} \quad n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a) + (-a)}_{(-n)\text{-φορές}}, & \text{όταν} \quad n < 0 \\ 0_R\,, & \text{όταν} \quad n = 0 \end{cases}$$

από τη θεωρία των προσθετικών αβελιανών ομάδων, τότε

$$(na)\, b = a\, (nb) = n(a\, b)$$

για όλα τα $n \in \mathbb{Z}$ *και όλα τα* $a, b \in R$.

(vi) *Εάν ο δακτύλιος R έχει μοναδιαίο στοιχείο και διαθέτει περισσότερα τού ενός στοιχεία, τότε* $1_R \neq 0_R$.

ΑΠΟΔΕΙΞΗ. (i) $0_R\, a = (0_R + 0_R)\, a = 0_R\, a + 0_R\, a \Longrightarrow 0_R\, a = 0_R$. Ομοίως δείχνει κανείς ότι $a\, 0_R = 0_R$.

(ii) Προφανώς, $a\, b + a\, (-b) = a\, (b + (-b)) = a\, 0_R = 0_R \Longrightarrow a\, (-b) = -(a\, b)$. Η δεύτερη ισότητα αποδεικνύεται με ανάλογο τρόπο.

(iii) Προφανώς, $(-a)\, (-b) = -(-a)\, b = -(-(a\, b)) = a\, b$ [ύστερα από διπλή εφαρμογή τής (ii)].

(iv) Θεωρούμε το m ως παγιωμένο και χρησιμοποιούμε μαθηματική επαγωγή ως προς τον n. Για $n = 1$ η ανωτέρω ισότητα γράφεται ως

$$(a_1 + \cdots + a_m)\, b_1 = a_1 b_1 + \cdots + a_m b_1$$

και είναι αληθής λόγω τής επιμεριστικής ιδιότητας τού πολλαπλασιασμού τού R ως προς την πρόσθεση. Ας υποθέσουμε ότι, για δοθέντες m, n, ισχύει η ισότητα

$$\left(\sum_{j=1}^{m} a_j\right)\, \left(\sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k.$$

Εφαρμόζοντας εκ νέου την επιμεριστική ιδιότητα, σε συνδυασμό με την επαγωγική μας υπόθεση, λαμβάνουμε

$$\begin{aligned}
&\left(\sum_{j=1}^{m} a_j\right)\, \left(\sum_{k=1}^{n+1} b_k\right) = \left(\sum_{j=1}^{m} a_j\right)\, \left(\sum_{k=1}^{n} b_k + b_{n+1}\right) \\
&= \left(\sum_{j=1}^{m} a_j\right)\, \left(\sum_{k=1}^{n} b_k\right) + \left(\sum_{j=1}^{m} a_j\right) b_{n+1} \\
&= \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k + \sum_{j=1}^{m} a_j\, b_{n+1} = \sum_{j=1}^{m} \sum_{k=1}^{n+1} a_j\, b_k.
\end{aligned}$$

(v) Τούτο έπεται άμεσα από το (iv).

(vi) Επί τη βάσει τής υποθέσεώς μας, $R \setminus \{0_R\} \neq \varnothing$. Άρα για κάθε $a \in R \setminus \{0_R\}$ έχουμε $1_R a = a$, οπότε $1_R \neq 0_R$. □

1.1.6 Ορισμός. Για κάθε στοιχείο a ενός δακτυλίου R και έναν $n \in \mathbb{N}$, θέτουμε

$$\boxed{a^n := \underbrace{a \cdot a \cdot \cdots\cdot a \cdot a}_{n \text{ φορές}}}$$

και $a^0 := 1_R$, όταν ο R διαθέτει μοναδιαίο στοιχείο. Προφανώς $a^m a^n = a^{m+n}$ και $(a^m)^n = a^{mn}$ για όλους τους φυσικούς αριθμούς m, n.

1.1.7 Πρόταση. (Διωνυμικοί τύποι) *Για κάθε μη αρνητικό ακέραιο αριθμό n ας συμβολίσουμε ως $n!$ το παραγοντικό τού n, όταν $n \geq 1$, θέτοντας $0! = 1$,*

και ως $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *τον διωνυμικό συντελεστή τού* n *υπεράνω τού* k*, όπου* $k \in \mathbb{Z}$*,* $0 \leq k \leq n$*. Υποθέτοντας ότι ο* R *είναι ένας δακτύλιος με μοναδιαίο στοιχείο, ο* n *ένας παγιωμένος φυσικός αριθμός, και (για κάποιον* $\nu \in \mathbb{N}$*) τα* $a, b, a_1, a_2, \ldots, a_\nu$*, στοιχεία τού* R*, έχουμε*:

(i) *Εάν* $ab = ba$*, τότε*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k} \tag{1.5}$$

(ii) *Εάν* $a_i a_j = a_j a_i$ *για όλους τους δείκτες* $1 \leq i, j \leq \nu$*, τότε*

$$(a_1 + a_2 + \cdots + a_\nu)^n = \sum \frac{n!}{(i_1!)\,(i_2!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} \tag{1.6}$$

όπου το άθροισμα λαμβάνεται υπεράνω όλων των ν*-άδων* $(i_1, i_2, \ldots, i_\nu) \in (\mathbb{N}_0)^\nu$ *για τις οποίες ισχύει* $i_1 + i_2 + \cdots + i_\nu = n$*.*

ΑΠΟΔΕΙΞΗ. (i) Θα χρησιμοποιήσουμε την «τριγωνική ταυτότητα τού Pascal», ήτοι την:

$$\tbinom{n}{j} + \tbinom{n}{j+1} = \tbinom{n+1}{j+1} \tag{1.7}$$

για κάθε $j, 0 \leq j < n$, και θα εργασθούμε με μαθηματική επαγωγή ως προς τον n. Για $n = 0$ η (1.5) είναι προφανής. Υποθέτοντας ότι η (1.5) είναι αληθής για κάποιον $n \geq 1$, λαμβάνουμε μέσω τής επιμεριστικής ιδιότητας:

$$\begin{aligned}
&(a+b)^{n+1} = (a+b)\sum_{k=0}^{n}\tbinom{n}{k} a^k\, b^{n-k}\\
&= \sum_{k=0}^{n}\tbinom{n}{k} a^{k+1}\, b^{n-k} + \sum_{k=0}^{n}\tbinom{n}{k} a^k\, b^{n-k+1} \quad [\text{επειδή } ab = ba]\\
&= \tbinom{n}{n} a^{n+1} + \sum_{k=0}^{n-1}\tbinom{n}{k}\, a^{k+1}\, b^{n-k} + \sum_{k=1}^{n}\tbinom{n}{k}\, a^k\, b^{n-k+1} + \tbinom{n}{0} b^{n+1}\\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1}\tbinom{n}{j}\, a^{j+1}\, b^{(n+1)-(j+1)} +\\
&+ \sum_{j=0}^{n-1}\tbinom{n}{j+1}\, a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1}\\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1}\left(\tbinom{n}{j} + \tbinom{n}{j+1}\right) a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1}\\
&\overset{(1.7)}{=} \tbinom{n+1}{n+1} a^{n+1} + \sum_{j=0}^{n-1}\tbinom{n+1}{j+1} a^{j+1}\, b^{(n+1)-(j+1)} + \tbinom{n+1}{0} b^{n+1}\\
&= \tbinom{n+1}{n+1} a^{n+1} + \sum_{k=0}^{n}\tbinom{n+1}{k} a^k\, b^{(n+1)-k} + \tbinom{n+1}{0} b^{n+1} = \sum_{k=0}^{n+1}\tbinom{n+1}{k} a^k\, b^{(n+1)-k}\,.
\end{aligned}$$

(ii) Για την απόδειξη τού τύπου (1.6) αρκεί να εφαρμόσουμε μαθηματική επαγωγή ως προς τον πληθικό αριθμό ν των προσθετέων. Για $\nu = 1$ ο (1.6) είναι προφανής,

ενώ για $\nu = 2$ συμπίπτει με τον (1.5), αφού

$$(a_1 + a_2)^n = \sum_{k=0}^{n} \tbinom{n}{k} a_1^k \, a_2^{n-k} = \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \tfrac{n!}{k!\; j!} \, a_1^k \, a_2^j \; .$$

Εάν υποθέσουμε ότι ο (1.6) είναι αληθής για κάποιον $\nu \geq 2$, τότε θα είναι αληθής και για τον $\nu + 1$, διότι

$$\begin{aligned} &(a_1 + a_2 + \cdots + a_\nu + a_{\nu+1})^n = ((a_1 + a_2 + \cdots + a_\nu) + a_{\nu+1})^n \\ &= \sum_{k=0}^{n} \tbinom{n}{k} (a_1 + \cdots + a_\nu)^k \, a_{\nu+1}^{n-k} = \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \tfrac{n!}{k!\; j!} \, (a_1 + \cdots + a_\nu)^k \, a_{\nu+1}^j \; , \end{aligned}$$

όπου το τελευταίο άθροισμα ισούται με

$$\begin{aligned} &\sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \tfrac{n!}{k!\; j!} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu : i_1+\cdots+i_\nu=k} \tfrac{k!}{(i_1!)\cdots(i_\nu!)} \, a_1^{i_1} \, a_2^{i_2} \, \cdots \, a_\nu^{i_\nu} \right) a_{\nu+1}^j \\ &= \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu : i_1+\cdots+i_\nu=k} \tfrac{n!k!}{k!\; j!(i_1!)\cdots(i_\nu!)} \, a_1^{i_1} \, a_2^{i_2} \, \cdots \, a_\nu^{i_\nu} a_{\nu+1}^j \right) \\ &= \sum_{(k,j)\in\mathbb{N}_0^2 : k+j=n} \left(\sum_{(i_1,..,i_\nu)\in(\mathbb{N}_0)^\nu : i_1+\cdots+i_\nu=k} \tfrac{n!}{(i_1!)\cdots(i_\nu!)(j!)} \, a_1^{i_1} \, a_2^{i_2} \, \cdots \, a_\nu^{i_\nu} a_{\nu+1}^j \right) \\ &= \sum_{(i_1,..,i_\nu,i_{\nu+1})\in(\mathbb{N}_0)^{\nu+1} : i_1+\cdots+i_\nu+i_{\nu+1}=n} \tfrac{n!}{(i_1!)\cdots(i_\nu!)(i_{\nu+1}!)} \, a_1^{i_1} \, a_2^{i_2} \, \cdots \, a_\nu^{i_\nu} a_{\nu+1}^{i_{\nu+1}} \end{aligned}$$

ύστερα από την αντικατάσταση τού αντιστοίχου τύπου για ν προσθετέους. □

1.1.8 Σημείωση. Δεδομένων των συνθηκών αμοιβαίας μεταθετικότητας των όρων μας, ανεπαίσθητες παραλλαγές των (1.5) και (1.6) παραμένουν ισχύουσες ακόμη και όταν ο δακτύλιος R *δεν* διαθέτει μοναδιαίο στοιχείο. Συγκεκριμένα, σε αυτήν την περίπτωση, μπορούμε να γράψουμε αντί τής (1.5),

$$(a + b)^n = a^n + \sum_{k=1}^{n-1} \tbinom{n}{k} a^k \, b^{n-k} + b^n$$

(και, αντιστοίχως, να μην εμφανίσουμε *καθόλου* στην (1.6) τους παράγοντες που είναι υψωμένοι στη μηδενική δύναμη). Ωστόσο, θα πρέπει να έχουμε πάντοτε στο νου μας ότι, όταν ένας δακτύλιος αναφοράς R δεν διαθέτει μοναδιαίο στοιχείο, το na, όπου $n \in \mathbb{Z}$ και $a \in R$, είναι στοιχείο τού R, *χωρίς* όμως το na να υποδηλοί -εν γένει- πολλαπλασιασμό δύο στοιχείων *εντός* τού R. Αντιθέτως, όταν ο R είναι δακτύλιος με μοναδιαίο, τότε το na υποδηλοί πάντοτε πολλαπλασιασμό δύο στοιχείων εντός τού R, καθότι αυτό γράφεται ως $na = (n \cdot 1_R)\, a$.

1.1.9 Ορισμός. Ένα μη κενό υποσύνολο S (τού υποκειμένου συνόλου R) ενός δακτυλίου $(R,+,\cdot)$ καλείται **υποδακτύλιος** τού $(R,+,\cdot)$ όταν το S είναι κλειστό ως προς αμφότερες τις πράξεις "$+$" και "$\cdot$" και καθίσταται αφ' εαυτού δακτύλιος (ως προς τον περιορισμό των εν λόγω πράξεων επ' αυτού).

1.1.10 Πρόταση. *Ένα μη κενό υποσύνολο S ενός δακτυλίου R είναι υποδακτύλιος τού R εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:*

(i) $a-b:=a+(-b)\in S$, *για κάθε* $a,b\in S$.

(ii) $ab\in S$, *για κάθε* $a,b\in S$.

1.1.11 Παραδείγματα. (i) Ο δακτύλιος $\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Q}$, ο $\mathbb{Q}$ υποδακτύλιος τού $\mathbb{R}$ και ο $\mathbb{R}$ είναι υποδακτύλιος τού $\mathbb{C}$. Επίσης, ο $2\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Z}$ και το $\{[0]_{10},[2]_{10},[4]_{10},[6]_{10},[8]_{10}\}$ υποδακτύλιος τού $\mathbb{Z}_{10}$.

(ii) Ο **δακτύλιος των ακεραίων τού Gauss (ή «γκαουσιανών ακεραίων»)**

$$\boxed{\mathbb{Z}[i]:=\{a+bi\mid a,b\in\mathbb{Z}\}\subsetneqq\mathbb{C}} \tag{1.8}$$

με πράξεις τις (συνήθεις πράξεις τού $\mathbb{C}$):

$$(a+bi)+(c+di):=(a+c)+(b+d)i,\ (a+bi)\cdot(c+di):=(ac-bd)+(ad+bc)i,$$

όπου i η «φανταστική» μονάδα, είναι (μεταθετικός) υποδακτύλιος τού δακτυλίου των μιγαδικών αριθμών, ενώ περιέχει τον $\mathbb{Z}$ ως υποδακτύλιό του. Γενικότερα, το

$$\boxed{\mathbb{Z}[\sqrt{m}]:=\{a+b\sqrt{m}\mid a,b\in\mathbb{Z}\}\subsetneqq\mathbb{C}} \tag{1.9}$$

όπου το $m\in\mathbb{Z}$ δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{|m|}\notin\mathbb{Q}$), καθίσταται υποδακτύλιος τού $\mathbb{R}$, όταν $m\in\mathbb{N}$, και υποδακτύλιος τού $\mathbb{C}$, όταν $m\in\mathbb{Z}\smallsetminus\mathbb{N}_0$, καθότι για οιουσδήποτε $a+b\sqrt{m}$, $a'+b'\sqrt{m}\in\mathbb{Z}[\sqrt{m}]$, έχουμε

$$\begin{cases}(a+b\sqrt{m})-(a'+b'\sqrt{m})=(a-a')+(b-b')\sqrt{m}\in\mathbb{Z}[\sqrt{m}],\\ (a+b\sqrt{m})\,(a'+b'\sqrt{m})=(aa'+bmb')+(ab'+ba')\sqrt{m}\in\mathbb{Z}[\sqrt{m}].\end{cases}$$

(iii) Κάθε δακτύλιος R έχει πάντοτε ως υποδακτυλίους τον εαυτό του και τον **τετριμμένο υποδακτύλιο** $\{0_R\}$. Ένας υποδακτύλιος S ενός δακτυλίου R με $S\subsetneqq R$ λέγεται **γνήσιος υποδακτύλιος** τού R.

1.1.12 Σημείωση. Έστω S ένας υποδακτύλιος ενός δακτυλίου R. Εάν ο R είναι μεταθετικός, τότε είναι προφανές ότι και ο S είναι μεταθετικός. Ωστόσο, εάν ο R είναι μη μεταθετικός και ο S *γνήσιος* υποδακτύλιός του, ο S ενδέχεται να είναι μεταθετικός, όπως, π.χ., συμβαίνει στην περίπτωση όπου

$$S:=\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in R\;\middle|\;b=c=0\right\},\ R:=\mathrm{Mat}_{2\times2}(\mathbb{Z}).$$

1.1.13 Σημείωση. Υπάρχουν υποδακτύλιοι S δακτυλίων R που συμπεριφέρονται αρκετά παράξενα όσον αφορά στην ύπαρξη ή μη μοναδιαίου στοιχείου.

(i) Ο S είναι δυνατόν να μην έχει μοναδιαίο στοιχείο, ενώ ο R να έχει, όπως π.χ. συμβαίνει στους $S = 2\mathbb{Z},\ R = \mathbb{Z}$.

(ii) Επίσης, ο S μπορεί να έχει μοναδιαίο στοιχείο, ενώ ο R να μην έχει, όπως π.χ. συμβαίνει στους $S = \{0\} \times \mathbb{R},\ R = 2\mathbb{Z} \times \mathbb{R}$.

(iii) Εάν ο R έχει μοναδιαίο στοιχείο το 1_R και $1_R \in S$, τότε $1_R = 1_S$.

(iv) Τέλος, ενδέχεται και οι δυο τους να έχουν μοναδιαία στοιχεία 1_S και 1_R, αντιστοίχως, χωρίς αυτά να είναι ίσα μεταξύ τους. Π.χ., ο $R = \mathbb{Z} \times \mathbb{Z}$ έχει ως μοναδιαίο του στοιχείο το $(1, 1)$, ενώ ο υποδακτύλιός του $S = \mathbb{Z} \times \{0\}$ το $(1, 0)$.

1.1.14 Πρόταση. *Εάν η $(S_j)_{j\in J}$ είναι μια μη κενή οικογένεια υποδακτυλίων ενός δακτυλίου R, τότε η τομή $\bigcap\limits_{j\in J} S_j$ αποτελεί έναν υποδακτύλιο τού R.*

ΑΠΟΔΕΙΞΗ. Επειδή $0_R \in S_j$ για κάθε $j \in J$, έχουμε $0_R \in \bigcap\limits_{j\in J} S_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $a, b \in \bigcap\limits_{j\in J} S_j$, τότε

$$[a, b \in S_j,\ \forall j \in J] \Longrightarrow [a - b \in S_j,\ \forall j \in J] \Longrightarrow a - b \in \bigcap_{j\in J} S_j$$

και $[a, b \in S_j,\ \forall j \in J] \Longrightarrow [ab \in S_j,\ \forall j \in J] \Longrightarrow ab \in \bigcap\limits_{j\in J} S_j$. Άρα η $\bigcap\limits_{j\in J} S_j$ είναι όντως ένας υποδακτύλιος τού R. (Βλ. πρόταση 1.1.10). □

1.1.15 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $S \subseteq R$ ένας υποδακτύλιος αυτού έχων ως μοναδιαίο του στοιχείο το 1_R. Εάν $\varnothing \neq A \subseteq R$, τότε (μέσω τής προτάσεως 1.1.14) ορίζεται ο *ελάχιστος* (ως προς τη σχέση τού συνολοθεωρητικού εγκλεισμού) υποδακτύλιος

$$S[A] := \bigcap \left\{ U \;\middle|\; \begin{array}{c} U \text{ υποδακτύλιος τού } R \\ \text{με } S \subseteq U \text{ και } A \subseteq U \end{array} \right\}$$

τού R (έχων ως μοναδιαίο του στοιχείο το 1_R) που περιέχει τόσον το υποσύνολο A όσον και τον S (ως υποδακτύλιό του). Λέμε ότι ο $S[A]$ είναι ο **υποδακτύλιος τού** R **(ή η επέκταση τού** S **εντός τού** R**) που προκύπτει ύστερα από προσάρτηση τού** A **στον** S. Στην ειδική περίπτωση όπου το A είναι ένα *πεπερασμένο* υποσύνολο $\{a_1, ..., a_k\}$ τού R, τότε αντί τού $S[A]$ γράφουμε απλώς $S[a_1, ..., a_k]$.

1.1.16 Πρόταση. *Εάν στον ορισμό* 1.1.15 *ο S είναι μεταθετικός και το $a \in R$ ένα στοιχείο, τέτοιο ώστε να ισχύει $as = sa$ για κάθε $s \in S$, τότε*

$$S[a] = \left\{ \sum_{j=0}^{\nu} s_j a^j \;\middle|\; \nu \in \mathbb{N}_0 \text{ και } s_0, ..., s_\nu \in S \right\}. \tag{1.10}$$

ΑΠΟΔΕΙΞΗ. Επειδή ο S είναι (εξ υποθέσεως) μεταθετικός και $as = sa$ για κάθε $s \in S$, το σύνολο $T := \left\{ \sum_{j=0}^{\nu} s_j a^j \middle| \nu \in \mathbb{N}_0 \text{ και } s_0, ..., s_\nu \in S \right\}$ (λόγω τής προτάσεως 1.1.10) είναι ένας υποδακτύλιος τού R ο οποίος περιέχει το $1_S = 1_R$. Επειδή $a = (1_S)a \in T$ και $S \subseteq T$ (διότι $s_0 a^0 = s_0(1_R) = s_0$ για κάθε $s_0 \in S$), έχουμε $S[a] \subseteq T$. Από την άλλη μεριά, είναι προφανές ότι ο T οφείλει να περιέχεται σε κάθε υποδακτύλιο τού R στον οποίο ανήκουν τα $1_R, a$ και S. Επομένως, $T \subseteq S[a]$ και η ισότητα (1.10) είναι αληθής. □

1.1.17 Παράδειγμα. Εάν $R = \mathbb{Q}$ και $S = \mathbb{Z}$, τότε $\mathbb{Z}[\frac{1}{5}] = \left\{ \frac{k}{5^n} \middle| k \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$.

1.1.18 Παραδείγματα. Όταν $R = \mathbb{C}$ και $S = \mathbb{Z}$, χαρακτηριστικά παραδείγματα είναι τα εξής:

(i) Για $a = i$ (όπου i η «φανταστική» μονάδα) λαμβάνουμε τον δακτύλιο (1.8) των γκαουσιανών ακεραίων. (Ως εκ τούτου, ο $\mathbb{Z}[i]$ είναι ο ελάχιστος υποδακτύλιος τού $\mathbb{C}$ που περιέχει τα i και $\mathbb{Z}$.) Γενικότερα, εάν το $m \in \mathbb{Z}$ δεν είναι τέλειο τετράγωνο, τότε για $a = \sqrt{m}$ λαμβάνουμε τον δακτύλιο (1.9). (Ως εκ τούτου, ο $\mathbb{Z}[\sqrt{m}]$ είναι ο ελάχιστος υποδακτύλιος τού $\mathbb{C}$ που περιέχει τα $\sqrt{m}$ και $\mathbb{Z}$.)

(ii) Εάν $\zeta_n := \exp\left(\frac{2\pi i}{n}\right) = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right), \forall n \in \mathbb{N}$, τότε για $n \geq 3$ και $a = \zeta_n$ λαμβάνουμε τον δακτύλιο

$$\mathbb{Z}[\zeta_n] = \left\{ \sum_{j=0}^{n-2} s_j \zeta_n^j \middle| s_0, ..., s_{n-2} \in \mathbb{Z} \right\},$$

διότι $\zeta_n^j = \zeta_n^i$, όταν $j > n$ και $j \equiv i (\mathrm{mod}\, n)$, $0 \leq i < n$, και $\zeta_n^{n-1} = -\sum_{k=0}^{n-2} \zeta_n^k$.

1.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

1.2.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα στοιχείο $a \in R \setminus \{0_R\}$ καλείται **δεξιός** (και αντιστοίχως, **αριστερός**) **μηδενοδιαιρέτης** όταν υπάρχει ένα $b \in R \setminus \{0_R\}$ (αντ. $c \in R \setminus \{0_R\}$), τέτοιο ώστε $ba = 0_R$ (και αντιστοίχως, $ac = 0_R$). Ένα στοιχείο τού[9] $R \setminus \{0_R\}$ καλείται **αμφίπλευρος μηδενοδιαιρέτης** ή απλώς **μηδενοδιαιρέτης** όταν αυτό είναι ταυτοχρόνως και δεξιός και αριστερός μηδενοδιαιρέτης. Το σύνολο όλων των μηδενοδιαιρετών ενός δακτυλίου R θα συμβολίζεται ως $\mathrm{Zdv}(R)$.

1.2.2 Παράδειγμα. Στον δακτύλιο $\mathrm{Mat}_{2\times 2}(R)$, όπου R ένας δακτύλιος με μοναδιαίο στοιχείο, έχουμε

$$\begin{pmatrix} 0_R & 0_R \\ 1_R & 0_R \end{pmatrix} \in \mathrm{Zdv}\left(\mathrm{Mat}_{2\times 2}(R)\right)$$

[9] Προσοχή! Ορισμένοι συγγραφείς συγκαταλέγουν *και το* 0_R στους μηδενοδιαιρέτες τού R (χαρακτηρίζοντάς το ως τον «τετριμμένο» μηδενοδιαιρέτη τού R). Ωστόσο, τούτη η *σύμβαση* **δεν** θα υιοθετηθεί εδώ!

διότι

$$\begin{pmatrix} 1_R & 0_R \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} 0_R & 0_R \\ 1_R & 0_R \end{pmatrix} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix},$$

και

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

1.2.3 Παρατήρηση. Στους *μεταθετικούς* δακτυλίους κάθε αριστερός μηδενοδιαιρέτης είναι δεξιός και αντιστρόφως. Ως εκ τούτου, δεν χρειάζεται να γίνεται διάκριση μεταξύ των δύο αυτών εννοιών.

1.2.4 Πρόταση. *Στον δακτύλιο $\mathbb{Z}_m$, $m \geq 1$, έχουμε*

$$\boxed{\mathrm{Zdv}\left(\mathbb{Z}_m\right) = \left\{[k]_m \in \mathbb{Z}_m \mid 1 \leq k \leq m-1,\ \ \mu\kappa\delta\left(k,m\right) > 1\right\}}$$

ΑΠΟΔΕΙΞΗ. Όταν $m = 1$, η ισότητα είναι προφανής, αφού $\mathrm{Zdv}(\mathbb{Z}_m) = \varnothing$. Από εδώ και στο εξής θα υποθέτουμε ότι $m \geq 2$.

" $\supseteq$ " Έστω $[k]_m \in \mathbb{Z}_m$, όπου $1 \leq k \leq m-1$, με $d := \mu\kappa\delta(k,m) > 1$. Τότε

$$\begin{aligned} [k]_m\,([m/d]_m) &= [km/d]_m = [(k/d)\,m]_m = [k/d\,]_m\,[m]_m \\ &= [k/d\,]_m\,[0]_m = [0]_m \Longrightarrow [k]_m \in \mathrm{Zdv}\left(\mathbb{Z}_m\right)\,. \end{aligned}$$

" $\subseteq$ " Αυτό θα προκύψει άμεσα από την κάπως γενικότερη πρόταση 1.2.17. □

1.2.5 Πρόταση. (Νόμος διαγραφής) *Έστω R ένας δακτύλιος. Τότε ο R δεν έχει δεξιούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο εξής νόμος τής διαγραφής*:

$$ca = cb \Longrightarrow a = b.$$

Κατ' αναλογίαν, ο R δεν έχει αριστερούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο ακόλουθος νόμος τής διαγραφής:

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

Κατά συνέπειαν, ο R δεν έχει ούτε δεξιούς ούτε αριστερούς μηδενοδιαιρέτες εάν και μόνον εάν για όλα τα στοιχεία $a, b \in R$ και όλα τα $c \in R \setminus \{0_R\}$ ισχύει ο εξής νόμος τής διαγραφής:

$$[ca = cb \quad \text{ή} \quad ac = bc] \Longrightarrow a = b.$$

(*Στους μεταθετικούς δακτυλίους οι δύο πρώτοι νόμοι διαγραφής ενσωματώνονται προδήλως σε έναν.*)

ΑΠΟΔΕΙΞΗ. Εάν ο R είναι ένας δακτύλιος χωρίς δεξιούς (και αντιστοίχως, χωρίς αριστερούς) μηδενοδιαιρέτες και $c \in R \setminus \{0\}$, τότε η ισότητα $ca = cb$ (και αντιστοίχως, η ισότητα $ac = bc$) γράφεται ως $c(a-b) = 0_R$ (και αντιστοίχως, ως $(a-b)c = 0_R$), πράγμα που σημαίνει ότι $a - b = 0_R$, δηλαδή $a = b$. Και αντιστρόφως· προϋποθέτοντας την ισχύ τού πρώτου (και αντιστοίχως, τού δεύτερου) εκ των νόμων τής διαγραφής, αρκεί να δείξουμε ότι για οιαδήποτε στοιχεία $c, d \in R$, η $cd = 0_R$ σημαίνει ότι $[c \neq 0_R \Longrightarrow d = 0_R]$ (και αντιστοίχως, ότι $[d \neq 0_R \Longrightarrow c = 0_R]$). Πράγματι· εάν $c \neq 0_R$, τότε έχουμε $cd = 0_R = c \cdot 0_R$, οπότε από τον πρώτο νόμο τής διαγραφής λαμβάνουμε $d = 0_R$, ενώ εάν $d \neq 0_R$, τότε η $cd = 0_R = 0_R \cdot d$ μας δίδει (κατ' αναλογίαν, μέσω τού δεύτερου νόμου τής διαγραφής) $c = 0_R$. □

1.2.6 Παράδειγμα. Στον δακτύλιο $\mathbb{Z}_6$ δεν ισχύει ο νόμος τής διαγραφής. (Σημειωτέον ότι $[2]_6\,[3]_6 = [6]_6 = [0]_6$, οπότε οι $[2]_6$ και $[3]_6$ είναι μηδενοδιαιρέτες. Μάλιστα, σύμφωνα με την πρόταση 1.2.4, $\mathrm{Zdv}(\mathbb{Z}_6) = \{[2]_6, [3]_6, [4]_6\}$.)

1.2.7 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο[10] $1_R \neq 0_R$. Ένα στοιχείο $a \in R$ καλείται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **αντιστρέψιμο** όταν $\exists b \in R$ (και αντιστοίχως, $\exists c \in R$), τέτοιο ώστε $ba = 1_R$ (και αντιστοίχως, $ac = 1_R$). Ένα τέτοιο $b \in R$ (αντ. $c \in R$) λέγεται **αριστερό** (και αντιστοίχως, **δεξιό**) **αντίστροφο**[11] τού a. Ένα στοιχείο τού R καλείται **αμφιπλεύρως αντιστρέψιμο** ή απλώς **αντιστρέψιμο** όταν αυτό είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών αντιστρέψιμο. Το σύνολο όλων των αντιστρεψίμων στοιχείων ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θα συμβολίζεται ως $R^\times$.

1.2.8 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $a \in R^\times$. Εάν το a διαθέτει το b ως ένα αριστερό αντίστροφό του και το c ως ένα δεξιό αντίστροφό του, τότε $b = c$.*

ΑΠΟΔΕΙΞΗ. Χρησιμοποιώντας τις ισότητες $ba = 1_R = ac$ συμπεραίνουμε άμεσα ότι $c = 1_R c = (ba)c = b(ac) = b\,1_R = b$. □

1.2.9 Συμβολισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $a \in R^\times$. Τότε υπάρχει κάποιο στοιχείο τού R, ας το πούμε b, τέτοιο ώστε $ba = 1_R = ab$ (επί τη βάσει τού ορισμού 1.2.7 και τής προτάσεως 1.2.8). Το b είναι *το μόνο* στοιχείο τού R που πληροί αυτήν την ιδιότητα, διότι για οιοδήποτε $b' \in R$ με $b'a = 1_R = ab'$ έχουμε $b = b'$ (αφού το b είναι αριστερό αντίστροφο και το b'

[10] Η συνθήκη $1_R \neq 0_R$ ισοδυναμεί με το ότι ο R δεν είναι τετριμμένος (βλ. 1.1.4 (vi)). Πράγματι· εάν $1_R = 0_R$, τότε για κάθε $a \in R$ έχουμε $a = 1_R \cdot a = 0_R \cdot a = 0_R$, οπότε ο R οφείλει να είναι τετριμμένος. Το αντίστροφο είναι προφανές.

[11] Προσοχή! Η ύπαρξη ενός αριστερού αντιστρόφου ενός $a \in R$ δεν εγγυάται *αυτομάτως* την ύπαρξη κάποιου δεξιού αντιστρόφου του και τανάπαλιν. Επίσης, δεν αποκλείεται ένα παγιωμένο $a \in R$ να διαθέτει δεξιά (και αντιστοίχως, αριστερά) αντίστροφα *περισσότερα τού ενός*. Τούτα (όπως δείχνεται στα εδάφια 1.2.8 και 1.2.9) αλλάζουν άρδην όταν περιοριζόμαστε στα *(αμφιπλεύρως) αντιστρέψιμα* στοιχεία.

δεξιό αντίστροφο τού a και τανάπαλιν). Αυτό το b καλείται **αντίστροφο στοιχείο τού** a και θα συμβολίζεται εφεξής ως a^{-1}. (Προφανώς, $1_R^{-1} = 1_R$, $\{\pm 1_R\} \subseteq R^\times$, $0_R \notin R^\times$ και για κάθε $a \in R^\times$ έχουμε $-a \in R^\times$ με $(-a)^{-1} = -a^{-1}$.) Επίσης, για κάθε στοιχείο $a \in R^\times$ και κάθε $n \in \mathbb{N}$, θα γράφουμε εν συντομία $a^{-n} := (a^{-1})^n$. (Πρβλ. 1.1.6).

1.2.10 Πρόταση. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Τότε το ζεύγος $(R^\times, \cdot)$ αποτελεί μια πολλαπλασιαστική ομάδα.*

ΑΠΟΔΕΙΞΗ. Επειδή $1_R \in R^\times$, έχουμε $R^\times \neq \varnothing$. Επιπροσθέτως, για οιαδήποτε $a, b \in R^\times$ έχουμε

$$\left(b^{-1}a^{-1}\right) ab = 1_R = ab\left(b^{-1}a^{-1}\right) \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \Rightarrow ab \in R^\times$$

(με $(ab)^{-1} = b^{-1}a^{-1}$) και $a^{-1}a = 1_R = aa^{-1} \Rightarrow a^{-1} \in R^\times$. Κατά συνέπειαν, το ζεύγος $(R^\times, \cdot)$ αποτελεί μια πολλαπλασιαστική ομάδα (με το 1_R ως ουδέτερο στοιχείο της). □

1.2.11 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Η ομάδα $R^\times$ καλείται **ομάδα των αντιστρεψίμων στοιχείων τού** R.

1.2.12 Σημείωση. (i) Η $R^\times$ είναι δυνατόν να είναι αβελιανή ακόμη και όταν ο R δεν είναι μεταθετικός, πρβλ. άσκηση **1-26** (v)).

(ii) Άλλοτε η $R^\times$ έχει *πεπερασμένη* τάξη, όπως στην περίπτωση θεωρήσεως τού δακτυλίου $R = \mathbb{Z}_m$, $m \geq 2$, με $\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid 1 \leq k \leq m-1,\ \text{μκδ}\,(k, m) = 1\}$ και $|\mathbb{Z}_m^\times| = \phi(m)$, όπου ϕ η συνάρτηση τού Euler, και άλλοτε *άπειρη*. Επί παραδείγματι, η

$$\mathbb{Z}[\sqrt{2}]^\times = \left\{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\right\}$$

είναι άπειρη αριθμήσιμη (βλ. σημείωση 5.2.41) και η $(\text{Mat}_{n\times n}(\mathbb{R}))^\times$ άπειρη υπεραριθμήσιμη (βλ. πρόταση 1.2.14).

(iii) Εάν ο S είναι ένας μη τετριμμένος υποδακτύλιος (με μοναδιαίο στοιχείο 1_S) ενός δακτυλίου R με μοναδιαίο στοιχείο $1_R = 1_S$, τότε $S^\times \subseteq R^\times \cap S$, χωρίς να αποκλείεται ο εγκλεισμός να είναι αυστηρός. Επί παραδείγματι, όταν $R = \mathbb{R}$ και $S = \mathbb{Z}$, τότε $2 \in R^\times = \mathbb{R}\setminus\{0\}$ αλλά $2 \notin S^\times = \{\pm 1\}$.

(iv) Εάν ο S είναι ένας μη τετριμμένος υποδακτύλιος (με μοναδιαίο στοιχείο 1_S) ενός δακτυλίου R με μοναδιαίο στοιχείο $1_R \neq 1_S$, τότε ενδέχεται να υπάρχει κάποιο στοιχείο τού S που είναι αντιστρέψιμο εντός τού S και μη αντιστρέψιμο εντός τού R. Επί παραδείγματι, όταν $R := \text{Mat}_{2\times 2}(\mathbb{R})$ και $S := \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \middle| x \in \mathbb{R} \right\}$, τότε

$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = 1_S$$

και για κάθε $x \in \mathbb{R}\setminus\{0\}$ έχουμε

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = 1_S = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix},$$

οπότε

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in S^\times \text{ και } \begin{pmatrix} x & x \\ x & x \end{pmatrix} \notin R^\times \cap S = \{\mathbf{A} \in S \mid \det(\mathbf{A}) \neq 0\} (= \varnothing),$$

όπου ως $\det(\mathbf{A})$ συμβολίζουμε την ορίζουσα τού $\mathbf{A}$.

1.2.13 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Η ομάδα των αντιστρεψίμων πινάκων

$$\boxed{\mathbf{GL}_n(R) := (\mathrm{Mat}_{n\times n}(R))^\times}$$

τού $\mathrm{Mat}_{n\times n}(R)$ καλείται, ιδιαιτέρως, **γενική γραμμική ομάδα (βαθμού n υπεράνω τού R)**.

1.2.14 Πρόταση. *Για κάθε μη τετριμμένο μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο και για κάθε $n \in \mathbb{N}$ ισχύει η ισότητα*

$$\boxed{\mathbf{GL}_n(R) = \{\mathbf{A} \in \mathrm{Mat}_{n\times n}(R) \mid \det(\mathbf{A}) \in R^\times\}.} \tag{1.11}$$

Επιπροσθέτως, για κάθε $\mathbf{A} \in \mathbf{GL}_n(R)$,

$$\boxed{\det(\mathbf{A}^{-1}) = \det(\mathbf{A})^{-1}} \tag{1.12}$$

και για $n \geq 2$,

$$\boxed{\mathbf{A}^{-1} = \det(\mathbf{A})^{-1}\mathbf{adj}(\mathbf{A}),} \tag{1.13}$$

όπου ως $\det(\mathbf{A})$ συμβολίζουμε την ορίζουσα τού $\mathbf{A}$ και ως $\mathbf{adj}(\mathbf{A})$ τον πίνακα τον προσαρτημένο στον $\mathbf{A}$.

ΑΠΟΔΕΙΞΗ. Για $n = 1$ οι (1.11) και (1.12) είναι προφανείς. Ας υποθέσουμε ότι $n \geq 2$ και ότι $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ και $\det(\mathbf{A}) \in R^\times$. Θέτοντας $\mathbf{B} := \det(\mathbf{A})^{-1}\mathbf{adj}(\mathbf{A})$ λαμβάνουμε μέσω τής (1.23) (τού (viii) τής ασκήσεως **1-19**) ότι

$$\mathbf{AB} = \mathbf{I}_n = \mathbf{BA} \Rightarrow \mathbf{A} \in \mathbf{GL}_n(R).$$

Και αντιστρόφως· εάν $\mathbf{A} \in \mathbf{GL}_n(R)$, τότε υπάρχει αντίστροφο στοιχείο $\mathbf{A}^{-1}$ τού $\mathbf{A}$. Κατά το (vi) τής ασκήσεως **1-19**,

$$\mathbf{A}\,\mathbf{A}^{-1} = \mathbf{I}_n = \mathbf{A}^{-1}\,\mathbf{A} \Rightarrow \det(\mathbf{A}) \cdot \det(\mathbf{A}^{-1}) = 1_R = \det(\mathbf{A}^{-1}) \cdot \det(\mathbf{A}),$$

οπότε $\det(\mathbf{A}) \in R^\times$ και $\det(\mathbf{A})^{-1} = \det(\mathbf{A}^{-1})$. (Η ισότητα (1.13) έπεται άμεσα από την (1.23).) □

1.2.15 Ορισμός. Ένα στοιχείο a ενός δακτυλίου R λέγεται **μηδενοδύναμο** όταν ισχύει $a^n = 0_R$ για κάποιον $n \in \mathbb{N}$. Το σύνολο όλων των μηδενοδυνάμων στοιχείων τού R θα συμβολίζεται ως $\mathrm{Nil}(R)$. (Ως **δείκτης** ενός $a \in \mathrm{Nil}(R)$ ορίζεται ο $\nu := \min\{\, n \in \mathbb{N} |\, a^n = 0_R\}$.)

1.2.16 Παράδειγμα. Στον δακτύλιο $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ έχουμε

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R \Rightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathrm{Nil}\,(R) \text{ (με δείκτη } 2).$$

1.2.17 Πρόταση. *Για κάθε μη τετριμμένο δακτύλιο R με μοναδιαίο στοιχείο ισχύουν οι εγκλειστικές σχέσεις*:

$$\boxed{\{1_R\} \subseteq R^\times \subseteq R \smallsetminus \mathrm{Zdv}(R) \subseteq (R \smallsetminus \mathrm{Nil}(R)) \cup \{0_R\} \subseteq R}$$

και

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

ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $a \in \mathrm{Nil}(R) \smallsetminus \{0_R\}$. Εάν το a έχει δείκτη ν, τότε (προφανώς) $a^{\nu-1} \neq 0_R$ και $a^\nu = a^{\nu-1}\, a = a\, a^{\nu-1} = 0_R \Longrightarrow a \in \mathrm{Zdv}(R)$. Έστω τώρα ότι $b \in \mathrm{Zdv}(R)$, δηλαδή ότι υπάρχουν $c, d \in R \smallsetminus \{0_R\}$ με $cb = bd = 0_R$. Εάν υποθέσουμε ότι $b \in R^\times$, τότε θα υπάρχουν στοιχεία $e, g \in R$, τέτοια ώστε $eb = bg = 1_R$. Αυτό όμως μας οδηγεί σε ένα άτοπο συμπέρασμα, αφού

$$\begin{aligned} 0_R &= (0_R)\, g = (cb)\, g = c\,(bg) = c\,(1_R) = c, \quad \text{ή} \\ 0_R &= e\,(0_R) = e\,(bd) = (eb)\, d = (1_R)\, d = d\,. \end{aligned}$$

Επομένως, $\mathrm{Zdv}(R) \cap R^\times = \varnothing$. Οι λοιπές εγκλειστικές σχέσεις είναι προφανείς. □

1.2.18 Ορισμός. (i) Κάθε μεταθετικός μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $\mathrm{Zdv}(R) = \varnothing$ καλείται **ακεραία περιοχή**[12]**.**

(ii) Κάθε μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $R^\times = R \smallsetminus \{0_R\}$ καλείται **διαιρετικός**[13] **δακτύλιος ή στρεβλό σώμα**[14]**.**

(iii) Κάθε μεταθετικός διαιρετικός δακτύλιος καλείται **σώμα.**

[12]Προφανώς, ένας μη τετριμμένος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο είναι ακεραία περιοχή εάν και μόνον εάν σε αυτόν ισχύει ο νόμος τής διαγραφής (βλ. πρόταση 1.2.5) ή, ισοδυνάμως, εάν και μόνον εάν από την ισότητα $ab = 0_R$ (όπου $a, b \in R$) έπεται κατ' ανάγκην ότι είτε $a = 0_R$ είτε $b = 0_R$.

[13]Η ονομασία «διαιρετικός δακτύλιος» (ή «δακτύλιος με διαίρεση») προέρχεται από το γεγονός τού ότι σε τέτοιου είδους δακτυλίους ορίζεται πάντοτε το ab^{-1}, *για κάθε* $a \in R$ και $b \in R \smallsetminus \{0_R\}$.

[14]Προφανώς, ο πληθικός αριθμός τού υποκειμένου συνόλου μιας ακεραίας περιοχής ή ενός στρεβλού σώματος R είναι ≥ 2 (αφού περιέχει τόσον το 1_R όσον και το $0_R (\neq 1_R)$).

1.2.19 Παραδείγματα. (i) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ αποτελούν σώματα. Από την άλλη μεριά, όπως είδαμε στα 1.1.4 (ii) και 1.2.2, ο δακτύλιος $\mathrm{Mat}_{2\times 2}(R)$, όπου το R είναι ένας εκ των $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, δεν μπορεί να είναι ούτε καν ακεραία περιοχή.

(ii) Έστω $\mathbb{H}_{\mathbb{R}} := \left\{ a\mathbf{I} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \;\middle|\; (a,b,c,d) \in \mathbb{R}^4 \right\}$ ο υποδακτύλιος τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ ο οριζόμενος μέσω των πραγματικών γραμμικών συνδυασμών των τεσσάρων πινάκων[15]

$$\mathbf{I} := \mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{j} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \mathbf{k} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \mathbf{i} := \mathbf{jk} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ο $\mathbb{H}_{\mathbb{R}}$ γράφεται ως εξής:

$$\boxed{\mathbb{H}_{\mathbb{R}} = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \;\middle|\; (a,b,c,d) \in \mathbb{R}^4 \right\}.}$$

Ο $\mathbb{H}_{\mathbb{R}}$ έχει το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{C})} = \mathbf{I}$ ως μοναδιαίο του στοιχείο. Ωστόσο, *δεν* είναι μεταθετικός, διότι π.χ. $\mathbf{i} \neq -\mathbf{i} = \mathbf{kj}$. Θεωρώντας ένα στοιχείο του

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

ένας τουλάχιστον εκ των a, b, c, d οφείλει να είναι $\neq 0$, πράγμα που σημαίνει ότι και η ορίζουσά του, η οποία ισούται με $a^2+b^2+c^2+d^2$, θα είναι $\neq 0$. Προφανώς, ο αντίστροφός του πίνακας

$$\tfrac{1}{a^2+b^2+c^2+d^2} \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix} \in \left(\mathrm{Mat}_{2\times 2}(\mathbb{C})\right)^{\times}$$

ανήκει στην ομάδα $\mathbb{H}_{\mathbb{R}}^{\times}$. Άρα ο $\mathbb{H}_{\mathbb{R}}$ αποτελεί έναν *διαιρετικό δακτύλιο*[16], ο οποίος ονομάζεται **δακτύλιος των τετρανίων**[17] **υπεράνω τού σώματος**[18] $\mathbb{R}$.

1.2.20 Πρόταση. *Κάθε μη τετριμμένος υποδακτύλιος S μιας ακεραίας περιοχής R, για τον οποίον $1_R \in S$, είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Επειδή $S \subseteq R$, έχουμε $1_S = 1_R$ και $\mathrm{Zdv}(S) \subseteq \mathrm{Zdv}(R) = \varnothing$. □

[15] Η λεγόμενη **ομάδα Q των τετρανίων**, η οποία παράγεται από τα στοιχεία $\mathbf{j}$ και $\mathbf{k}$, υπεισέρχεται ουσιωδώς στην ταξινόμηση των πεπερασμένων ομάδων τάξεως 8.

[16] Ο $\mathbb{H}_{\mathbb{R}}$ είναι εφοδιασμένος και με τη δομή ενός *τετραδιάστατου πραγματικού διανυσματικού χώρου*, αφού οι πίνακες $\mathbf{I}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ είναι και γραμμικώς ανεξάρτητοι υπεράνω τού $\mathbb{R}$.

[17] Τα «τετράνια» επινοήθηκαν από τον William Royal Hamilton (1805-1865) το έτος 1843 ως ένα αλγεβρικό σύστημα περιέχον το σώμα $\mathbb{C}$ των μιγαδικών αριθμών (γι' αυτό λέγονται και «υπερμιγαδικοί αριθμοί»). Το στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$, πέραν τής συχνής χρήσεώς του στη Διανυσματική Ανάλυση, υπεισέρχεται και σε εφαρμογές τόσον τής σύγχρονης Αλγεβρικής Τοπολογίας όσον και τής Μαθηματικής Φυσικής.

[18] Ενίοτε, εκτός τού ιδίου τού $\mathbb{H}_{\mathbb{R}}$, χρησιμοποιούνται (σε διάφορες εφαρμογές) και υποδακτύλιοι αυτού

$$\mathbb{H}_R := \left\{ a\mathbf{I} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \;\middle|\; (a,b,c,d) \in R^4 \right\} \subseteq \mathbb{H}_{\mathbb{R}}$$

οριζόμενοι υπεράνω διαφόρων υποδακτυλίων R τού σώματος $\mathbb{R}$. (Τα στοιχεία τού $\mathbb{H}_{\mathbb{Z}}$ καλούνται, ιδιαιτέρως, **ακέραια τετράνια** και τού $\mathbb{H}_{\mathbb{Q}}$ **ρητά τετράνια**.)

1.2.21 Παρατήρηση. Ο υποδακτύλιος $2\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}$ *δεν* είναι ακεραία περιοχή, παρότι $\mathrm{Zdv}(2\mathbb{Z}) = \varnothing$, αφού δεν διεθέτει μοναδιαίο στοιχείο.

1.2.22 Πόρισμα. *Κάθε μη τετριμμένος υποδακτύλιος S ενός σώματος K, για τον οποίον $1_K \in S$, είναι ακεραία περιοχή.* (*Ειδικότερα, κάθε σώμα είναι ακεραία περιοχή.*)

1.2.23 Παράδειγμα. Υπάρχουν ακέραιες περιοχές που δεν είναι σώματα. Τα απλούστερα παραδείγματα μας τα παρέχουν ο δακτύλιος $\mathbb{Z}$ των ακεραίων (με τις συνήθεις πράξεις), αφού $\mathrm{Zdv}(\mathbb{Z}) = \varnothing$ και $\mathbb{Z}^\times = \{-1, +1\} \subsetneqq \mathbb{Z}\setminus\{0\}$, και ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. άσκηση **1-43**), αφού $\mathrm{Zdv}(\mathbb{Z}[i]) = \varnothing$ και $\mathbb{Z}[i]^\times = \{-1, +1, -i, i\} \subsetneqq \mathbb{Z}[i]\setminus\{0\}$. Από την άλλη μεριά, για *πεπερασμένους* μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο $1_R \neq 0_R$ οι έννοιες ακεραία περιοχή και σώμα ταυτίζονται. (Βλ. πρόταση 1.2.26).

1.2.24 Σημείωση. Εάν R είναι μια ακεραία περιοχή και ο S υποδακτύλιός της με μοναδιαίο στοιχείο, ο οποίος συμβαίνει να είναι ακεραία περιοχή ως προς τις ίδιες πράξεις, τότε ο S καλείται **υποπεριοχή** τής ακεραίας περιοχής R. (Όταν ο S είναι υποπεριοχή τής R, έχουμε κατ' ανάγκην $1_S = 1_R$. Βλ. άσκηση **1-24**.) Επί παραδείγματι, το $R := \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$ (ως προς τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ρητών αριθμών) είναι υποπεριοχή τού $\mathbb{Q}$ και $\mathbb{Z} \subsetneqq R \subseteq \mathbb{Q}$. (Βλ. άσκηση **1-31**).

1.2.25 Σημείωση. Εάν το L είναι ένα σώμα και το K ένας υποδακτύλιος τού L με μοναδιαίο στοιχείο, ο οποίος συμβαίνει να είναι σώμα ως προς τις ίδιες πράξεις, τότε το K καλείται **υπόσωμα** τού L και το L (σωματική) **επέκταση** τού K. (Εν τοιαύτη περιπτώσει, $1_L = 1_K$.) Επί παραδείγματι, το $\mathbb{Q}$ είναι υπόσωμα τού $\mathbb{R}$ και το $\mathbb{R}$ υπόσωμα τού $\mathbb{C}$.

1.2.26 Πρόταση. *Κάθε πεπερασμένος μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, ο οποίος δεν διαθέτει ούτε αριστερούς ούτε δεξιούς μηδενοδιαιρέτες, είναι διαιρετικός. Ειδικότερα, κάθε πεπερασμένη ακεραία περιοχή είναι σώμα.*

ΑΠΟΔΕΙΞΗ. Έστω R ένας πεπερασμένος μη τετριμμένος δακτύλιος χωρίς δεξιούς ή αριστερούς μηδενοδιαιρέτες και $a \in R\setminus\{0_R\}$. Αρκεί να προσδιορισθεί ένα στοιχείο $b \in R$ με $ab = ba = 1_R$. Θεωρούμε την απεικόνιση $\beta : R \to R$, την οριζόμενη μέσω τής $\beta(c) := ac$ (και, αντιστοίχως, μέσω τής $\beta(c) := ca$) για όλα τα $c \in R$. Σύμφωνα με τον νόμο τής διαγραφής 1.2.5, για $c, c' \in R$ με $\beta(c) = \beta(c')$, λαμβάνουμε $c = c'$. Άρα η β, ως ενριπτική απεικόνιση, θα είναι και επιρριπτική. Αυτό σημαίνει ότι για το 1_R θα υπάρχει ένα αρχέτυπο μέσω τής β, δηλαδή ένα $b \in R$, τέτοιο ώστε $\beta(b) = 1_R$. (Όπως έχουμε ήδη προαναφέρει, τα αριστερά και δεξιά αντίστροφα ενός αντιστρεψίμου στοιχείου a ενός τέτοιου R ταυτίζονται.) □

1.2.27 Πόρισμα. *Οι ακόλουθες συνθήκες για τον δακτύλιο $\mathbb{Z}_m$, $m \geq 2$, είναι ισοδύναμες:*

(i) *Ο m είναι πρώτος αριθμός.*

(ii) *Ο $\mathbb{Z}_m$ είναι μια ακεραία περιοχή.*

(iii) *Ο $\mathbb{Z}_m$ αποτελεί ένα σώμα.*

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή (i) $\Rightarrow$ (ii) έπεται από την πρόταση 1.2.4, η (ii) $\Rightarrow$ (iii) από την πρόταση 1.2.26, και η (iii) $\Rightarrow$ (ii) από την πρόταση 1.2.22. Τέλος, για τη συνεπαγωγή (ii) $\Rightarrow$ (i) ας υποθέσουμε ότι ο m είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $m = pq$ δύο άλλων ακεραίων p, q, όπου $1 < p, q < m$. Αυτό θα σήμαινε ότι $[m]_m = [0]_m = [p]_m [q]_m$ με $p \neq 0$ και $q \neq 0$, πράγμα που αντίκειται στην (ii). □

1.2.28 Θεώρημα. (Wedderburn, 1905) *Κάθε πεπερασμένος διαιρετικός δακτύλιος είναι σώμα.*[19]

ΑΠΟΔΕΙΞΗ. Βλ. T.W. Hungerford: *Algebra*, Graduate Texts in Math., Vol. **73**, Springer-Verlag, fifth printing, 1989, Ch. IX, Cor. 6.9, p. 462. □

1.2.29 Ορισμός. Έστω L ένα σώμα και έστω $K \subseteq L$ ένα υπόσωμα αυτού. Εάν $\varnothing \neq A \subseteq L$, τότε ορίζεται το *ελάχιστο* (ως προς τη σχέση τού συνολοθεωρητικού εγκλεισμού) υπόσωμα

$$\boxed{K(A) := \bigcap \{U \,|U \text{ υπόσωμα τού } L \text{ με } K \cup A \subseteq U\}}$$

τού L που περιέχει τόσον το υποσύνολο A όσον και το K. (Πρβλ. άσκηση **1-42**.) Λέμε ότι το $K(A)$ είναι το **υπόσωμα τού L (ή η επέκταση τού K εντός τού L) που προκύπτει ύστερα από προσάρτηση τού A στο K**. Στην ειδική περίπτωση όπου το A είναι ένα *πεπερασμένο* υποσύνολο $\{a_1, ..., a_k\}$ τού L, τότε αντί τού $K(A)$ γράφουμε απλώς $K(a_1, ..., a_k)$.

1.2.30 Σημείωση. Λαμβάνοντας υπ' όψιν τον ορισμό 1.1.15, διαπιστώνουμε ότι $K[A] \subseteq K(A)$, ήτοι ότι ο *υποδακτύλιος* $K[A]$ τού L που προκύπτει ύστερα από προσάρτηση τού A στο K περιέχεται (ενδεχομένως και γνησίως) εντός τού *υποσώματος* $K(A)$ τού L που προκύπτει ύστερα από προσάρτηση τού A στο K (διότι ο δακτύλιος $K[A]$ δεν είναι κατ' ανάγκην σώμα).

1.2.31 Παραδείγματα. (i) Έστω m ένας ακέραιος αριθμός που δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{|m|} \notin \mathbb{Q}$). Είναι εύκολο να δειχθεί ότι ο υποδακτύλιος[20]

$$\boxed{\mathbb{Q}[\sqrt{m}] = \{r + s\sqrt{m} \mid r, s \in \mathbb{Q}\} \subsetneqq \mathbb{C}} \tag{1.14}$$

[19] Για την αρχική απόδειξη βλ. J.H.M. Wedderburn: *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349-352.

[20] Η ισότητα (1.14) προκύπτει άμεσα από την (1.10).

τού σώματος $\mathbb{C}$ που προκύπτει ύστερα από προσάρτηση τού $\sqrt{m}$ στο $\mathbb{Q}$ είναι *υπόσωμα* τού $\mathbb{C}$ (βλ. το (iv) τής ασκήσεως **1-44**), οπότε[21]

$$\boxed{\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m}).}$$

Σημειωτέον ότι ισχύουν οι ακόλουθοι εγκλεισμοί:

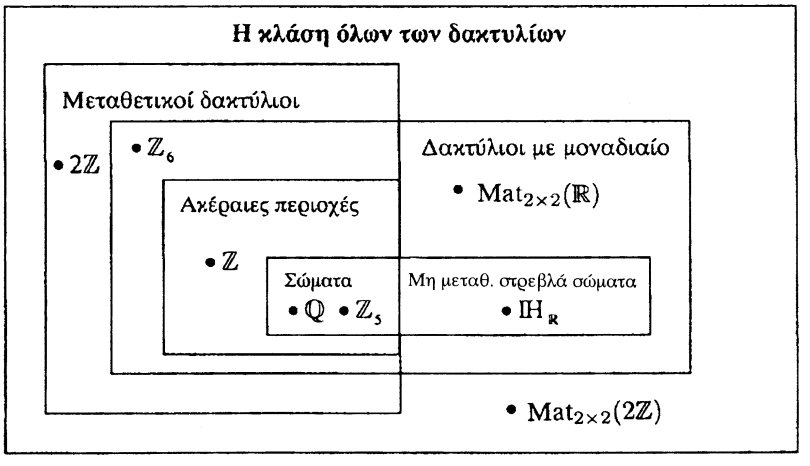
$$\mathbb{Z} \subsetneqq \mathbb{Z}[\sqrt{m}] \subsetneqq \mathbb{Q}(\sqrt{m}), \quad \mathbb{Z} \subsetneqq \mathbb{Q} \subsetneqq \mathbb{Q}(\sqrt{m}).$$

(ii) Αντιθέτως, για τον υποδακτύλιο τού σώματος $\mathbb{R}$ που προκύπτει ύστερα από προσάρτηση τού $\pi = 3,14159...$ (ήτοι τού λόγου τού μήκους τής περιφέρειας ενός κύκλου προς τη διάμετρό του) στο $\mathbb{Q}$ έχουμε

$$\boxed{\mathbb{Q}[\pi] \underset{(1.10)}{=} \left\{ \sum_{j=0}^{\nu} r_j \pi^j \,\middle|\, \nu \in \mathbb{N}_0 \text{ και } r_0, ..., r_\nu \in \mathbb{Q} \right\} \subsetneqq \mathbb{Q}(\pi),}$$

διότι $\pi^{-1} \in \mathbb{Q}(\pi) \setminus \mathbb{Q}[\pi]$ (λόγω τής υπερβατικότητας τού π).

1.2.32 Σημείωση. Κατά τα προαναφερθέντα, είναι εφικτή μια υποδιαίρεση τής κλάσεως όλων των δακτυλίων σε υποκλάσεις, βασιζόμενη σε έννοιες απορρέουσες από τις πρωταρχικές ιδιότητες τής πολλαπλασιαστικής πράξεως, την ύπαρξη ή μη μηδενοδιαιρετών και το «εύρος» τής πολλαπλασιαστικής ομάδας των αντιστρεψίμων στοιχείων. Οι εν λόγω υποκλάσεις, καθώς και χαρακτηριστικά παραδείγματα δακτυλίων ανήκοντα σε κάθε μία εξ αυτών, καταχωρίζονται στο ακόλουθο διάγραμμα:



[21] Αυτό το σώμα μπορεί να ιδωθεί και ως υπόσωμα τού σώματος $\mathbb{R}$ των πραγματικών αριθμών όταν $m > 0$.

1.3 ΔΑΚΤΥΛΙΟΙ ΠΟΛΥΩΝΥΜΩΝ ΚΑΙ ΕΠΙΤΥΠΩΝ ΔΥΝΑΜΟΣΕΙΡΩΝ

Δοθέντος ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θεωρούμε το σύνολο $R^{\mathbb{N}_0}$ όλων των ακολουθιών $(a_0, a_1, a_2, \dots\dots)$ με τα $a_i \in R$, $i = 0, 1, 2, \dots$, καθώς και το σύνολο $R^{(\mathbb{N}_0)}$ όλων των ακολουθιών $(a_0, a_1, a_2, \dots\dots)$ με τα $a_i \in R$, $i = 0, 1, 2, \dots$, για τις οποίες υπάρχουν *το πολύ πεπερασμένου πλήθους* a_i που είναι διάφορα τού 0_R. Κάθε στοιχείο φ τού $R^{(\mathbb{N}_0)}$ γράφεται υπό τη μορφή

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

για κάποιον ακέραιο αριθμό $n \geq 0$. Προφανώς, δυο στοιχεία

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

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

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

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0, \; \forall m \in \mathbb{N}_0. \tag{1.15}$$

Η τριάδα $(R^{\mathbb{N}_0}, +, \cdot)$ αποτελεί έναν δακτύλιο με μηδενικό του στοιχείο το $(0_R, 0_R, \dots)$ και μοναδιαίο του στοιχείο το $(1_R, 0_R, 0_R, \dots)$ και η τριάδα $(R^{(\mathbb{N}_0)}, +, \cdot)$ έναν υποδακτύλιο τού $(R^{\mathbb{N}_0}, +, \cdot)$ (με μοναδιαίο στοιχείο του το $(1_R, 0_R, 0_R, \dots)$). Επίσης, *ταυτίζοντας* κάθε $a \in R$ με το $(a, 0_R, 0_R, \dots)$ έχουμε τη δυνατότητα θεωρήσεως τού $(R, +, \cdot)$ ως έναν υποδακτύλιο τού $(R^{(\mathbb{N}_0)}, +, \cdot)$. Εισάγοντας ένα νέο σύμβολο

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

παρατηρούμε ότι, βάσει των ως άνω πράξεων,

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

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

και, γενικότερα,

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

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

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

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

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

Κατ' αναλογίαν, εάν το $(a_0, a_1, a_2, \dots)$ είναι τυχόν στοιχείο τού δακτυλίου $R^{(\mathbb{N}_0)}$, όπου $a_i = 0_R$,για κάθε $i > n$, για κάποιον παγιωμένο $n \in \mathbb{N}_0$, τότε μπορούμε να γράψουμε

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

1.3.1 Ορισμός. (i) Ο δακτύλιος $R^{\mathbb{N}_0}$ συμβολίζεται συνήθως ως $R[\![\mathsf{X}]\!]$ και καλείται **δακτύλιος επίτυπων δυναμοσειρών** (ή **τύποις δυναμοσειρών**) μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **επίτυπες δυναμοσειρές** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \dots$ ονομάζονται **συντελεστές** των επίτυπων δυναμοσειρών.

(ii) Ο δακτύλιος $R^{(\mathbb{N}_0)}$ συμβολίζεται συνήθως ως $R\,[\mathsf{X}]$ και καλείται **δακτύλιος πολυωνύμων** (ή **πολυωνυμικός δακτύλιος**) μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **πολυώνυμα** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \dots$ ονομάζονται **συντελεστές** των πολυωνύμων.

1.3.2 Παρατήρηση. Βάσει τού ορισμού τού πολλαπλασιασμού πολυωνύμων (και αντιστοίχως, επίτυπων δυναμοσειρών) είναι σαφές ότι ο δακτύλιος $R[\mathsf{X}]$ (και αντιστοίχως, ο δακτύλιος $R[\![\mathsf{X}]\!]$) είναι μεταθετικός εάν και μόνον εάν ο ίδιος ο R είναι μεταθετικός.

1.3.3 Σημείωση. Εκ των ανωτέρω συμπεραίνουμε ότι δυο επίτυπες δυναμοσειρές

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

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

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

είναι **ίσα** ($\varphi(\mathsf{X}) = \psi(\mathsf{X})$) εάν και μόνον εάν *είτε* αμφότερα είναι ίσα με το $0_{R[\mathsf{X}]}$ *είτε*

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

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

1.3.4 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\} \;\; \text{και} \;\; n := \min\{\, k \in \mathbb{N}_0 |\, a_k \neq 0_R\},$$

τότε λέμε ότι ο αριθμός $\mathrm{ord}(\varphi(\mathsf{X})) := n$ είναι **η τάξη** τής επίτυπης δυναμοσειράς $\varphi(\mathsf{X})$ και το a_0 **ο σταθερός όρος** τής $\varphi(\mathsf{X})$. Στην περίπτωση όπου $\varphi(\mathsf{X}) = 0_{R[\![\mathsf{X}]\!]}$ είναι η **μηδενική επίτυπη δυναμοσειρά**, θέτουμε εξ ορισμού $\mathrm{ord}(\varphi(\mathsf{X})) := \infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[22]: $\infty > n, \;\; \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο η τάξη των επίτυπων δυναμοσειρών μπορεί να εκληφθεί ως μια απεικόνιση

$$\mathrm{ord} : R[\![\mathsf{X}]\!] \longrightarrow \mathbb{N}_0 \cup \{\infty\}\,.$$

1.3.5 Λήμμα. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!]$ ισχύουν τα εξής*:

(i) $\mathrm{ord}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \geq \min\{\mathrm{ord}(\varphi(\mathsf{X})), \mathrm{ord}(\psi(\mathsf{X}))\}$.

(ii) $\mathrm{ord}(\varphi(\mathsf{X})\psi(\mathsf{X})) \geq \mathrm{ord}(\varphi(\mathsf{X})) + \mathrm{ord}(\psi(\mathsf{X}))$.

(iii) *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ *και* $\mathrm{ord}(\varphi(\mathsf{X})) \neq \mathrm{ord}(\psi(\mathsf{X}))$, *τότε*

$$\mathrm{ord}\,(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = \min\{\mathrm{ord}\,(\varphi(\mathsf{X})), \mathrm{ord}(\psi(\mathsf{X}))\}.$$

(iv) *Εάν o R είναι ακεραία περιοχή, τότε*

$$\mathrm{ord}\,(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \mathrm{ord}\,(\varphi(\mathsf{X})) + \mathrm{ord}(\psi(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον μία εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι ίση με την $0_{R[\![\mathsf{X}]\!]}$, τότε τα (i), (ii) και (iv) είναι προφανώς αληθή. Αρκεί λοιπόν να υποθέσουμε ότι $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ και ότι

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i, \;\; n := \mathrm{ord}(\varphi(\mathsf{X})), \quad \psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i, \;\; m := \mathrm{ord}(\psi(\mathsf{X})).$$

(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n \leq m$. Τότε το άθροισμα $\varphi(\mathsf{X}) + \psi(\mathsf{X})$ ισούται με

$$\sum_{i=0}^{\infty} (a_i + b_i)\, \mathsf{X}^i = \begin{cases} a_n \mathsf{X}^n + \displaystyle\sum_{i=n+1}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n < m, \\ \displaystyle\sum_{i=n}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n = m, \end{cases} \tag{1.16}$$

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

οπότε[23] $\mathrm{ord}(\varphi(\mathsf{X})+\psi(\mathsf{X}))\geq n=\min\{\mathrm{ord}(\varphi(\mathsf{X}))\,,\,\mathrm{ord}(\psi(\mathsf{X}))\}$.

(ii) Βάσει τής (1.15) το γινόμενο των δύο επίτυπων δυναμοσειρών μπορεί να γραφεί ως

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

όπου

$$\sum_{i=0}^{k}a_ib_{k-i}=\begin{cases}a_nb_m, & \text{όταν } k=n+m,\\ 0_R, & \text{όταν } k\leq n+m-1.\end{cases}\tag{1.17}$$

Κατά συνέπειαν[24], $\mathrm{ord}(\varphi(\mathsf{X})\psi(\mathsf{X}))\geq n+m=\mathrm{ord}(\varphi(\mathsf{X}))+\mathrm{ord}(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n<m$. Τότε έχουμε $a_n+b_n=a_n\neq 0_R$ και από την (1.16) έπεται ότι

$$\mathrm{ord}\,(\varphi(\mathsf{X})+\psi(\mathsf{X}))=n=\min\{\mathrm{ord}\,(\varphi(\mathsf{X}))\,,\ \mathrm{ord}(\psi(\mathsf{X}))\}.$$

(iv) Επειδή $a_nb_m\neq 0_R$, λαμβάνουμε $\mathrm{ord}(\varphi(\mathsf{X})\psi(\mathsf{X}))=\mathrm{ord}(\varphi(\mathsf{X}))+\mathrm{ord}(\psi(\mathsf{X}))$ από την (1.17). □

1.3.6 Ορισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν

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

τότε λέμε ότι ο αριθμός $\deg(\varphi(\mathsf{X}))=n$ είναι **ο βαθμός** τού πολυωνύμου $\varphi(\mathsf{X})$, το a_0 **ο σταθερός όρος** τού $\varphi(\mathsf{X})$ και ο $\mathrm{LC}(\varphi(\mathsf{X}))=a_n$ ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού $\varphi(\mathsf{X})$. Όταν $\mathrm{LC}(\varphi(\mathsf{X}))=1_R$, τότε το $\varphi(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου $\varphi(\mathsf{X})=0_{R[\mathsf{X}]}$ είναι το **μηδενικό πολυώνυμο**, θέτουμε εξ ορισμού $\deg(\varphi(\mathsf{X}))=-\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[25]: $-\infty<n,\ \forall n\in\mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

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

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

[23] Προφανώς, αυτή ισχύει ως *γνήσια* ανισότητα εάν και μόνον εάν $n=m$ και $a_n=-b_n$.

[24] Αυτή ισχύει ως *γνήσια* ανισότητα εάν και μόνον εάν $a_nb_m=0_R$.

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

1.3.7 Λήμμα. *Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}]$ ισχύουν τα εξής*:

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

(ii) $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) \leq \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

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

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

(iv) *Εάν* $\mathrm{LC}(\varphi(\mathsf{X}))\cdot \mathrm{LC}(\psi(\mathsf{X})) \neq 0_R$, *τότε*

$$\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X})).$$

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

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

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

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

$$\varphi(\mathsf{X}) + \psi(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{1.18}$$

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

(ii) Βάσει τής (1.15) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

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

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0_R, & \text{όταν } k \geq n+m+1 \end{cases} \tag{1.19}$$

Κατά συνέπειαν, $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) \leq n + m = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (1.18) έπεται ότι

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

(iv) Επειδή $a_n b_m = \mathrm{LC}(\varphi(\mathsf{X}))\cdot \mathrm{LC}(\psi(\mathsf{X})) \neq 0_R$, από την ισότητα (1.19) λαμβάνουμε $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$. □

1.3.8 Παραδείγματα. Σημειωτέον ότι οι ανωτέρω ανισοϊσότητες μπορούν πράγματι να ισχύουν και ως αυστηρές ανισότητες.
(i) Εάν $\varphi(\mathsf{X}) = 2\mathsf{X} + 1$, $\psi(\mathsf{X}) = -2\mathsf{X} + 1 \in \mathbb{Z}\,[\mathsf{X}]$, τότε

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

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

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

που σημαίνει ότι $0 = \deg\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) < \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X})) = 2$.

1.3.9 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα εξής*:
(i) *Για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ έχουμε*

$$\deg\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X}))$$

και για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ έχουμε

$$\operatorname{ord}\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X})).$$

(ii) *Οι δακτύλιοι $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$ είναι ακέραιες περιοχές.*
(iii) *Έχουμε $R\,[\mathsf{X}]^\times = R^\times$ (ήτοι τα αντιστρέψιμα πολυώνυμα τού $R\,[\mathsf{X}]$ είναι τα σταθερά πολυώνυμα τής μορφής $\varphi(\mathsf{X}) = a_0 \in R^\times$) και*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]^\times \iff a_0 \in R^\times.$$

ΑΠΟΔΕΙΞΗ. (i)-(ii) Οι $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$ είναι μη τετριμμένοι, μεταθετικοί δακτύλιοι με μοναδιαίο τους στοιχείο το 1_R. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$, τότε

$$\operatorname{LC}(\varphi(\mathsf{X})) \cdot \operatorname{LC}(\psi(\mathsf{X})) \neq 0_R,$$

διότι ο R δεν διαθέτει μηδενοδιαιρέτες, οπότε από το 1.3.7 (iv) έχουμε

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

Συνεπώς, $\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, οπότε ούτε ο $R[\mathsf{X}]$ δεν έχει μηδενοδιαιρέτες. Εν συνεχεία θεωρούμε $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$. Από το 1.3.5 (iv) έχουμε

$$\operatorname{ord}\left(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})\right) = \operatorname{ord}\left(\varphi(\mathsf{X})\right) + \operatorname{ord}(\psi(\mathsf{X})) \in \mathbb{N}_0.$$

Συνεπώς, $\varphi(\mathsf{X}) \cdot \psi(\mathsf{X}) \neq 0_{R[\![\mathsf{X}]\!]}$, οπότε ούτε ο $R[\![\mathsf{X}]\!]$ δεν έχει μηδενοδιαιρέτες.
(iii) Εάν το $\varphi(\mathsf{X})$ είναι ένα αντιστρέψιμο στοιχείο τού $R[\mathsf{X}]$, τότε υπάρχει ένα πολυώνυμο $\psi(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιο ώστε να ισχύει $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_{R[\mathsf{X}]}$. Τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μη μηδενικά, καθότι $1_{R[\mathsf{X}]} = 1_R \neq 0_R = 0_{R[\mathsf{X}]}$. Από το (i) συνάγεται ότι

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

οπότε τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι κατ' ανάγκην αντιστρέψιμα στοιχεία τού R. Εάν τώρα

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

έχουμε

$$\varphi(\mathsf{X}) \in R[\![\mathsf{X}]\!]^\times \iff a_0 \in R^\times.$$

Πράγματι· εάν υπάρχει $\psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in R[\![\mathsf{X}]\!]$ με $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_R$, τότε $a_0 b_0 = 1_R$, οπότε $a_0 \in R^\times$. Και αντιστρόφως· εάν $a_0 \in R^\times$, τότε μπορούμε να προσδιορίσουμε διαδοχικώς $b_0, b_1, \ldots, b_i, b_{i+1}, \ldots \in R$, ούτως ώστε να ισχύουν οι ισότητες

$$\begin{cases} b_0 a_0 = 1_R, \\ b_1 a_0 + b_0 a_1 = 0_R, \\ \vdots \\ b_i a_0 + b_{i-1} a_1 + \cdots + b_0 a_i = 0_R, \\ \vdots \end{cases}$$

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

$$b_i := -a_0^{-1}(b_{i-1} a_1 + \cdots + b_0 a_i).$$

Θέτοντας $\psi(\mathsf{X}) := \sum_{i=0}^{\infty} b_i \mathsf{X}^i$, λαμβάνουμε $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_R$ και ο ισχυρισμός είναι αληθής. □

1.3.10 Πόρισμα. *Έστω K ένα σώμα. Τότε ισχύουν τα εξής*:
(i) *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_{K[\mathsf{X}]}\}$, τότε*

$$\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$$

και $K[\mathsf{X}]^\times = K^\times = K \setminus \{0_K\} = \{\varphi(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(\varphi(\mathsf{X})) = 0\}$.
(ii) *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \setminus \{0_{K[\![\mathsf{X}]\!]}\}$, τότε*

$$\operatorname{ord}(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \operatorname{ord}(\varphi(\mathsf{X})) + \operatorname{ord}(\psi(\mathsf{X}))$$

και

$$K[\![\mathsf{X}]\!]^\times = \{\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \mid \operatorname{ord}(\varphi(\mathsf{X})) = 0\}.$$

Επιπροσθέτως, κάθε επίτυπη δυναμοσειρά $\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \setminus \{0_{K[\![\mathsf{X}]\!]}\}$ γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \mathsf{X}^{\operatorname{ord}(\varphi(\mathsf{X}))} \chi(\mathsf{X}),$$

για κάποια (μονοσημάντως ορισμένη) επίτυπη δυναμοσειρά $\chi(\mathsf{X}) \in K[\![\mathsf{X}]\!]^\times$.

ΑΠΟΔΕΙΞΗ. Οι ισχυρισμοί περί των βαθμών τού γινομένου δύο μη μηδενικών πολυωνύμων, περί των τάξεων δύο μη μηδενικών επίτυπων δυναμοσειρών και περί των ομάδων των αντιστρεψίμων στοιχείων είναι προδήλως αληθείς βάσει των όσων απεδείχθησαν στην πρόταση 1.3.9. Έστω τώρα τυχούσα επίτυπη δυναμοσειρά

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

με $n := \mathrm{ord}(\varphi(\mathsf{X}))$. Θέτοντας $\chi(\mathsf{X}) := \sum\limits_{i=n}^{\infty} a_i \mathsf{X}^{i-n}$ λαμβάνουμε $\varphi(\mathsf{X}) = \mathsf{X}^n \chi(\mathsf{X})$. Η επίτυπη δυναμοσειρά $\chi(\mathsf{X}) \in K[\![\mathsf{X}]\!]$ είναι αντιστρέψιμη, διότι ο σταθερός της όρος a_n είναι $\neq 0_K$, οπότε ανήκει στην ομάδα $K^\times = K \setminus \{0_K\}$. □

1.3.11 Σημείωση. Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «απεικονίσεις» (επειδή εκεί γίνεται κυρίως χρήση των δακτυλίων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντες* δακτυλίους R με μοναδιαίο στοιχείο, κάτι τέτοιο *δεν* είναι εν γένει αληθές. Εάν $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]$, η **απεικόνιση η επαγομένη από το** $\varphi(\mathsf{X})$ είναι εξ ορισμού η

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

Όμως η $R[\mathsf{X}] \longrightarrow \mathrm{ΑΠ}(R,R) = R^R,\ \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}$, δεν είναι κατ' ανάγκην ένριψη. Επί παραδείγματι, εάν $R = \mathbb{Z}_3$ και

$$\varphi(\mathsf{X}) = [1]_3 \mathsf{X} + [1]_3 \mathsf{X}^3, \quad \psi(\mathsf{X}) = [2]_3 \mathsf{X},$$

τότε τα $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ -ως πολυώνυμα- είναι διαφορετικά (βλ. 1.3.3), ενώ

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

πράγμα που σημαίνει ότι $\mathfrak{v}_{\varphi(\mathsf{X})} = \mathfrak{v}_{\psi(\mathsf{X})}$.

► **Μετάβαση στις πολλές απροσδιορίστους**. Αυτή καθίσταται εφικτή ύστερα από επανάληψη τής διαδικασίας κατασκευής των $R[\mathsf{X}]$ και $R[\![\mathsf{X}]\!]$, όπου ο ίδιος ο R είναι ένας δακτύλιος πολυωνύμων και ένας δακτύλιος επίτυπων δυναμοσειρών, αντιστοίχως, ακολουθούμενη από αναδρομικό ορισμό.

1.3.12 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο.

(i) Ο δακτύλιος $(R[\![\mathsf{X}_1]\!])\,[\![\mathsf{X}_2]\!]$ των επίτυπων δυναμοσειρών μίας απροσδιορίστου

X_2 με συντελεστές ειλημμένους από τον $R[\![\mathsf{X}_1]\!]$ καλείται **δακτύλιος επίτυπων δυναμοσειρών δύο (ανεξαρτήτων) απροσδιορίστων** X_1 **και** X_2 με συντελεστές ειλημμένους από τον R και συμβολίζεται ως $R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$. Κάθε $\varphi(\mathsf{X}_1, \mathsf{X}_2) \in R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$ είναι τής μορφής

$$\varphi(\mathsf{X}_1, \mathsf{X}_2) = \sum_{(i,j)\in\mathbb{N}_0^2} a_{ij}\mathsf{X}_1^i\mathsf{X}_2^j, \;\; a_{ij} \in R.$$

Κατ' αναλογίαν, ο δακτύλιος $(R[\mathsf{X}_1])\,[\mathsf{X}_2]$ των πολυωνύμων μίας απροσδιορίστου X_2 με συντελεστές ειλημμένους από τον $R[\mathsf{X}_1]$ καλείται **δακτύλιος πολυωνύμων δύο (ανεξαρτήτων) απροσδιορίστων** X_1 **και** X_2 με συντελεστές ειλημμένους από τον R και συμβολίζεται ως $R[\mathsf{X}_1, \mathsf{X}_2]$. Κάθε στοιχείο $\varphi(\mathsf{X}_1, \mathsf{X}_2) \in R[\mathsf{X}_1, \mathsf{X}_2]$ είναι τής μορφής

$$\varphi(\mathsf{X}_1, \mathsf{X}_2) = \sum_{(i,j)\in\Lambda} a_{ij}\mathsf{X}_1^i\mathsf{X}_2^j, \;\; a_{ij} \in R, \; \Lambda \subseteq \mathbb{N}_0^2, \; \text{card}(\Lambda) < \infty.$$

(Προφανώς, ο $R[\mathsf{X}_1, \mathsf{X}_2]$ είναι υποδακτύλιος τού $R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$ και επί τη βάσει των συνήθων ταυτίσεων ισχύει $1_{R[\![\mathsf{X}_1,\mathsf{X}_2]\!]} = 1_{R[\mathsf{X}_1,\mathsf{X}_2]} = 1_R$.)

(ii) Γενικότερα, για οιονδήποτε φυσικό αριθμό $n \geq 2$, ο δακτύλιος $R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$ **επίτυπων δυναμοσειρών** n **(ανεξαρτήτων) απροσδιορίστων** $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από τον R ορίζεται αναδρομικώς ως

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

Κατ' αναλογίαν, ο **δακτύλιος** $R\,[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ **πολυωνύμων** n **(ανεξαρτήτων) απροσδιορίστων** $\mathsf{X}_1, \ldots, \mathsf{X}_n$ με συντελεστές ειλημμένους από τον R ορίζεται αναδρομικώς ως εξής[26]:

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

1.4 Η ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΤΩΝ ΔΑΚΤΥΛΙΩΝ

1.4.1 Ορισμός. Έστω R ένας δακτύλιος. Ας υποθέσουμε ότι υπάρχει ένας $m \in \mathbb{N}$ με την ιδιότητα

$$ma = 0_R, \quad \forall a \in R.$$

Εάν ο $n \in \mathbb{N}$ είναι ο ελάχιστος φυσικός αριθμός με αυτήν την ιδιότητα, τότε ο n λέγεται **χαρακτηριστική** τού δακτυλίου R. Εάν δεν υπάρχει κανένας $m \in \mathbb{N}$ με την ανωτέρω ιδιότητα, τότε λέμε ότι ο δακτύλιος R έχει **χαρακτηριστική** 0. Η χαρακτηριστική ενός δακτυλίου R θα συμβολίζεται ως $\text{χαρ}(R)$.

[26] Ο $R\,[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ (και αντιστοίχως, ο $R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$) είναι μεταθετικός εάν και μόνον εάν ο ίδιος ο R είναι μεταθετικός.

1.4.2 Παραδείγματα. (i) Οι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ έχουν χαρακτηριστική 0.
(ii) Ο $\mathbb{Z}_m$ έχει χαρακτηριστική m.
(iii) Προφανώς, $\text{χαρ}(R) = 1 \Longleftrightarrow$ ο R είναι τετριμμένος δακτύλιος.

1.4.3 Πρόταση. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε*

$$\text{χαρ}\,(R) = n > 0 \Longleftrightarrow n = \min\{m \in \mathbb{N} \mid m \cdot 1_R = 0_R\}.$$

ΑΠΟΔΕΙΞΗ. "$\Longrightarrow$" Εξ ορισμού, εάν ο R έχει χαρακτηριστική $n > 0$, τότε $na = 0_R$ για *κάθε* $a \in R$, οπότε $n \cdot 1_R = 0_R$. Εάν υπήρχε κάποιος ακέραιος m, $0 < m < n$, τέτοιος ώστε να ισχύει $m \cdot 1_R = 0_R$, τότε θα είχαμε

$$ma = m\,(1_R \cdot a) = (m \cdot 1_R)\,a = 0_R \cdot a = 0_R, \;\; \forall a \in R,$$

δηλαδή κάτι που θα αντέφασκε προς το γεγονός ότι ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $na = 0_R$ για κάθε $a \in R$.
"$\Longleftarrow$" Εάν ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $n \cdot 1_R = 0_R$, τότε για κάθε $a \in R$ έχουμε

$$na = n\,(1_R \cdot a) = (n \cdot 1_R)\,a = 0_R \cdot a = 0_R,$$

οπότε $\text{χαρ}(R) = k$, για κάποιον φυσικό αριθμό k, όπου $0 < k \leq n$. Επειδή όμως τότε θα ισχύει και η ισότητα $k \cdot 1_R = 0_R$, θα πρέπει (βάσει τής υποθέσεώς μας) να έχουμε $k = n$. □

1.4.4 Παράδειγμα. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Τότε

$$\text{χαρ}\,(R) = \text{χαρ}\,(R[\mathsf{X}]) = \text{χαρ}\,(R[\![\mathsf{X}]\!]).$$

Ας αποδείξουμε την πρώτη ισότητα. (Η απόδειξη τής δεύτερης είναι παρόμοια.)
Περίπτωση πρώτη. $\text{χαρ}(R[\mathsf{X}]) = n > 0$. Τότε $n = \min\{m \in \mathbb{N} | \, m \cdot 1_{R[\mathsf{X}]} = 0_{R[\mathsf{X}]}\}$. Επειδή το 1_R (και αντιστοίχως, το 0_R) ταυτίζεται (κατά τα ειωθότα) με το $1_{R[\mathsf{X}]}$ (και αντιστοίχως, με το $0_{R[\mathsf{X}]}$), λαμβάνουμε $\text{χαρ}(R) = n$.
Περίπτωση δεύτερη. Έστω ότι $\text{χαρ}(R[\mathsf{X}]) = 0$. Εάν υποθέταμε ότι $\text{χαρ}(R) = n > 0$, τότε (χρησιμοποιώντας την ίδια επιχειρηματολογία) θα είχαμε $\text{χαρ}(R[\mathsf{X}]) = n$ και θα καταλήγαμε σε άτοπο. Άρα $\text{χαρ}(R) = 0$.

1.4.5 Πρόταση. *Η χαρακτηριστική οιασδήποτε ακεραίας περιοχής R είναι είτε μηδέν είτε ένας πρώτος αριθμός.*

ΑΠΟΔΕΙΞΗ. Έστω ότι $\text{χαρ}(R) = n \neq 0$. Υποθέτουμε πως ο n είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $n = kl$ δύο φυσικών αριθμών k και l, όπου $1 < k, l < n$. Τότε $0_R = n \cdot 1_R = (kl) \cdot 1_R = (k \cdot 1_R)\,(l \cdot 1_R)$, και επειδή ο R δεν διαθέτει μηδενοδιαιρέτες λαμβάνουμε $(k \cdot 1_R) = 0_R$ ή $(l \cdot 1_R) = 0_R$, πράγμα που αντιφάσκει προς το γεγονός ότι ο n είναι ο *ελάχιστος* φυσικός αριθμός με αυτήν την ιδιότητα. (Βλ. πρόταση 1.4.3). Άρα τελικώς ο n οφείλει να είναι πρώτος αριθμός. □

1.4.6 Πρόταση. *Έστω R μια ακεραία περιοχή.*

(i) *Εάν* $\text{χαρ}(R) = 0$, *τότε κάθε μη μηδενικό στοιχείο τής προσθετικής ομάδας* $(R, +)$ *έχει άπειρη τάξη.*

(ii) *Εάν* $\text{χαρ}(R) = p$ *(*p *πρώτος), τότε κάθε μη μηδενικό στοιχείο τής προσθετικής ομάδας* $(R, +)$ *έχει τάξη* p.

ΑΠΟΔΕΙΞΗ. (i) Εάν $\text{χαρ}(R) = 0$ και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$ και υποθέσουμε πως αυτό είναι τάξεως $m \in \mathbb{N}$, τότε

$$0_R = ma = (m \cdot 1_R)\, a \Longrightarrow m \cdot 1_R = 0_R,$$

ήτοι κάτι το αδύνατο. Άρα το a οφείλει να έχει άπειρη τάξη.

(ii) Εάν $\text{χαρ}(R) = p$ (p πρώτος) και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$, τότε από τον ορισμό τής χαρακτηριστικής τού R προκύπτει ότι $\text{ord}(a) \leq p$. Όμως η ισότητα $0_R = \text{ord}(a)\, a = (\text{ord}\,(a) \cdot 1_R)\, a$ δίδει και πάλι $\text{ord}(a) \cdot 1_R = 0_R$ (διότι ο δακτύλιος R στερείται μηδενοδιαιρετών), πράγμα που σημαίνει ότι $\text{ord}(a) \geq p$ δυνάμει τής προτάσεως 1.4.3. Συνεπώς, $\text{ord}(a) = p$. □

1.4.7 Πόρισμα. *Εάν R είναι μια πεπερασμένη ακεραία περιοχή (ήτοι ένα πεπερασμένο σώμα), τότε η χαρακτηριστική της θα είναι ένας πρώτος αριθμός.*

1.4.8 Πρόταση. *Εάν R είναι μια ακεραία περιοχή με χαρακτηριστική έναν πρώτο αριθμό p, τότε για οιαδήποτε $a, b, a_1, \ldots, a_n \in R$ έχουμε*:

(i) $(a \pm b)^p = a^p \pm b^p$.

(ii) $(a \pm b)^{p^\nu} = a^{p^\nu} \pm b^{p^\nu}$ *για κάθε* $\nu \in \mathbb{N}$.

(iii) $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a_n^p$.

(iv) $(a_1 + \cdots + a_n)^{p^\nu} = a_1^{p^\nu} + \cdots + a_n^{p^\nu}$ *για κάθε* $\nu \in \mathbb{N}$.

Ασκήσεις

1-1. Έστω $(R, +, \cdot)$ ένας δακτύλιος. Χρησιμοποιώντας τόν συμβολισμό τον εισαχθέντα στα εδάφια 1.1.5 (v) και 1.1.6, να αποδειχθεί ότι ισχύουν οι ακόλουθες ισότητες:

(i) $n(ab) = (na)b$, για κάθε $n \in \mathbb{Z}$ και κάθε $(a, b) \in R \times R$.

(ii) $n(ab) = a(nb)$, για κάθε $n \in \mathbb{Z}$ και κάθε $(a, b) \in R \times R$.

(iii) $(ma)(nb) = (mn)(ab)$, για κάθε $(m, n) \in \mathbb{Z}^2$ και κάθε $(a, b) \in R \times R$.

(iv) $(ma)^n = m^n a^n$, για οιαδήποτε $m \in \mathbb{Z}$, $n \in \mathbb{N}$ και $a \in R$.

(v) $(-a)^{2n} = a^{2n}$, για κάθε $a \in R$ και για κάθε $n \in \mathbb{N}$ και

(vi) $(-a)^{2n+1} = -a^{2n+1}$, για κάθε $a \in R$ και για κάθε $n \in \mathbb{N}_0$.

1-2. Έστω $(R,+,\cdot)$ ένας δακτύλιος και έστω $(a,b)\in R\times R$. Εάν $ab=ba$, να αποδειχθεί ότι ισχύουν οι ακόλουθες ισότητες:

(i) $(a+b)^2=a^2+2ab+b^2$, $(a-b)^2=a^2-2ab+b^2$,

(ii) $a^2-b^2=(a-b)(a+b)=(a+b)(a-b)$,

(iii) Για κάθε φυσικό αριθμό $n\geq 3$,

$$\begin{aligned} a^n-b^n &= (a-b)\left(a^{n-1}+\sum_{j=2}^{n-1}a^{n-j}b^{j-1}+b^{n-1}\right)\\ &= \left(a^{n-1}+\sum_{j=2}^{n-1}a^{n-j}b^{j-1}+b^{n-1}\right)(a-b)\,, \end{aligned}$$

(iv) Για κάθε φυσικό αριθμό $n\geq 1$,

$$\begin{aligned} a^{2n+1}+b^{2n+1} &= (a+b)\left(a^{2n}-a^{2n-1}b+\cdots+a^2b^{2n-2}-ab^{2n-1}+b^{2n}\right)\\ &= \left(a^{2n}-a^{2n-1}b+\cdots+a^2b^{2n-2}-ab^{2n-1}+b^{2n}\right)(a+b)\,, \end{aligned}$$

(v) Για κάθε φυσικό αριθμό $n\geq 2$,

$$\begin{aligned} a^{2n}-b^{2n} &= (a+b)\left(a^{2n-1}-a^{2n-2}b+\cdots-a^2b^{2n-3}+ab^{2n-2}-b^{2n-1}\right)\\ &= \left(a^{2n-1}-a^{2n-2}b+\cdots-a^2b^{2n-3}+ab^{2n-2}-b^{2n-1}\right)(a+b)\,. \end{aligned}$$

1-3. Εάν $(m,n)\in\mathbb{N}\times\mathbb{N}$ με μκδ$(m,n)=1$ και a,b είναι αντιστρέψιμα στοιχεία ενός δακτυλίου R με μοναδιαίο στοιχείο, τέτοια ώστε να ισχύει $a^m=b^m$ και $a^n=b^n$, να αποδειχθεί ότι $a=b$.

1-4. Έστω $(R,+,\cdot)$ ένας δακτύλιος. Λέμε ότι ο δακτύλιος $(R,+,*)$ ο οριζόμενος επί τού συνόλου R, με την ίδια την "$+$" ως πράξη προσθέσεως και την

$$R\times R\ni(a,b)\longmapsto a*b:=b\cdot a\in R$$

ως πράξη πολλαπλασιασμού, είναι **ο αντικείμενος δακτύλιος τού** R. Εν συντομία, ο δακτύλιος αυτός συμβολίζεται συνήθως ως R^{opp}. Να αποδειχθούν τα ακόλουθα:

(i) $(R^{\text{opp}})^{\text{opp}}=R$.

(ii) $R^{\text{opp}}=R$ εάν και μόνον εάν ο R είναι μεταθετικός.

(iii) Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο R^{opp} έχει μοναδιαίο στοιχείο· επιπροσθέτως, $1_{R^{\text{opp}}}=1_R$.

1-5. Έστω R ένας δακτύλιος για τον οποίο ισχύει η ισότητα

$$x^2=x,\ \ \forall x\in R.$$

Να αποδειχθεί ότι $2x = 0_R,\ \forall x \in R$, και ότι ο εν λόγω δακτύλιος οφείλει να είναι μεταθετικός. Επιπροσθέτως, στην περίπτωση κατά την οποία ο R έχει τουλάχιστον τρία στοιχεία, να αποδειχθεί ότι ο R διαθέτει μηδενοδιαιρέτες. (Αυτού τού είδους οι δακτύλιοι ονομάζονται **δακτύλιοι τού Boole**).

1-6. Έστω R ένας δακτύλιος για τον οποίο ισχύει η ισότητα

$$x^2 = 2x,\ \ \forall x \in R.$$

Να αποδειχθεί ότι $x^3 = 0_R,\ \forall x \in R$.

1-7. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο για τον οποίο ισχύει η ισότητα

$$x^3 = x,\ \ \forall x \in R.$$

Να αποδειχθεί (i) ότι $6x = 0_R,\ \forall x \in R$, και (ii) ότι ο R είναι κατ' ανάγκην μεταθετικός.

1-8. Έστω R ένας δακτύλιος. Θέτοντας $[a, b] := ab - ba,\ \forall (a, b) \in R \times R$, να αποδειχθεί η **ταυτότητα τού Jacobi**:

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0_R,\ \forall (a, b, c) \in R \times R \times R.$$

1-9. Έστω M ένα μη κενό σύνολο και έστω $\mathfrak{P}(M)$ το δυναμοσύνολό του. Να αποδειχθεί ότι η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$, όπου

$$A \triangle B := (A \setminus B) \cup (B \setminus A),\ \forall (A, B) \in \mathfrak{P}(M) \times \mathfrak{P}(M),$$

η **συμμετρική διαφορά των** A **και** B, αποτελεί έναν μεταθετικό δακτύλιο τού Boole με μοναδιαίο στοιχείο.

1-10. Εάν η $(G, +)$ είναι μια προσθετική αβελιανή ομάδα, να αποδειχθεί ότι η τριάδα $(\mathrm{End}(G), +, \circ)$, όπου $\mathrm{End}(G)$ το σύνολο των ενδομορφισμών τής G, "$+$" η συνήθης (κατά σημείο) πρόσθεση και "$\circ$" η συνήθης πράξη τής συνθέσεως απεικονίσεων, αποτελεί έναν δακτύλιο με την id_G ως μοναδιαίο του στοιχείο.

1-11. Έστω p πρώτος αριθμός και $Q_p := \left\{ [a]_p^2 \;\middle|\; [a]_p \in \mathbb{Z}_p \right\}$ το σύνολο των τετραγώνων των στοιχείων τού $\mathbb{Z}_p$.

(i) Ποιος είναι ο πληθικός αριθμός $\mathrm{card}(Q_p)$ τού Q_p;

(ii) Να αποδειχθεί ότι το ζεύγος $(Q_p, +)$ είναι μια υποομάδα τής $(\mathbb{Z}_p, +)$ μόνον όταν $p = 2$.

(iii) Για οιαδήποτε $u, v \in \mathbb{Z}_p \setminus Q_p$, να αποδειχθεί ότι $uv \in Q_p$.

1-12. Έστω p πρώτος αριθμός. Να αποδειχθεί ότι κάθε στοιχείο τού $\mathbb{Z}_p$ *μπορεί να παρασταθεί ως άθροισμα τετραγώνων* δύο στοιχείων τού $\mathbb{Z}_p$. (*Υπόδειξη*: Να γίνει κατάλληλη χρήση τής ασκήσεως **1-11**.)

1-13. Να αποδειχθεί η πρόταση 1.1.10.

1-14. Εάν R είναι τυχών δακτύλιος, να αποδειχθεί ότι το $\{(r,r) \mid r \in R\}$ αποτελεί έναν υποδακτύλιο τού $R \times R$.

1-15. Να εξετασθεί ποια εκ των ακολούθων συνόλων είναι υποδακτύλιοι τού $\mathbb{Q}$:

(i) $S_1 := \left\{ r \in \mathbb{Q} \;\middle|\; \begin{array}{c} r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\}), \\ \text{με μκδ}\,(a,b) = 1 \text{ και } b \equiv 1 (\mathrm{mod}\, 2) \end{array} \right\}$.

(ii) $S_2 := \left\{ r \in \mathbb{Q} \;\middle|\; \begin{array}{c} r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\}), \\ \text{με μκδ}\,(a,b) = 1 \text{ και } b \equiv 0 (\mathrm{mod}\, 2) \end{array} \right\}$.

(iii) $S_3 := \left\{ r \in \mathbb{Q} \;\middle|\; \begin{array}{c} r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\}), \\ \text{με μκδ}\,(a,b) = 1 \text{ και } a \equiv 1 (\mathrm{mod}\, 2) \end{array} \right\}$.

(iv) $S_4 := \left\{ r \in \mathbb{Q} \;\middle|\; \begin{array}{c} r = \frac{a}{b},\ (a,b) \in \mathbb{Z}\times(\mathbb{Z}\setminus\{0\}), \\ \text{με μκδ}\,(a,b) = 1 \text{ και } a \equiv 0 (\mathrm{mod}\, 2) \end{array} \right\}$.

(v) $S_5 := \mathbb{Q}_{\geq 0} := \{ r \in \mathbb{Q} \mid r \geq 0 \}$.

(vi) $S_6 := \left\{ r^2 \;\middle|\; r \in \mathbb{Q} \right\}$.

1-16. Για οιονδήποτε πρώτο αριθμό p ορίζουμε το σύνολο

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

Να αποδειχθεί ότι το $\mathbb{Z}_{\langle p \rangle}$ είναι υποδακτύλιος τού $\mathbb{Q}$. (Το $\mathbb{Z}_{\langle p \rangle}$ ονομάζεται **δακτύλιος των p-αδικών κλασμάτων** και παίζει έναν ιδιαίτερο ρόλο στην Αλγεβρική Θεωρία Αριθμών.)

1-17. Να εξετασθεί ποια εκ των ακολούθων συνόλων είναι υποδακτύλιοι τού $\mathbb{R}^{[0,1]}$:

(i) $S_1 := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f(q) = 0, \forall q \in \mathbb{Q} \cap [0,1] \right\}$.

(ii) $S_2 := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; \begin{array}{c} f(x) = \sum_{j=0}^{\nu} s_j x^j, \forall x \in [0,1], \\ \text{όπου } \nu \in \mathbb{N}_0 \text{ και } s_0, ..., s_\nu \in \mathbb{R} \end{array} \right\}$.

(iii) $S_3 := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; \begin{array}{c} f(x) = 0 \text{ μόνον για} \\ \text{πεπερασμένου πλήθους } x \in [0,1] \end{array} \right\} \cup \{0_{\mathbb{R}^{[0,1]}}\}$.

(iv) $S_4 := \left\{ f \in \mathbb{R}^{[0,1]} \mid f(x) = 0 \text{ για άπειρα } x \in [0,1] \right\}$.

(v) $S_5 := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; \lim_{x \longrightarrow 1} f(x) = 0 \right\}$.

(vi) $S_6 := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; \begin{array}{c} f(x) = \sum_{i=1}^{k} r_i \sin(m_i x) + \sum_{j=1}^{l} s_j \cos(n_j x), \\ \text{για κάποιους } r_i, s_j \in \mathbb{Q} \text{ και } m_i, n_j \in \mathbb{N}_0,\ k, l \in \mathbb{N} \end{array} \right\}$.

1-18. Να προσδιορισθούν όλοι οι υποδακτύλιοι τού δακτυλίου $\mathbb{Z}_3 \times \mathbb{Z}_3$.

1-19. Εάν n είναι ένας φυσικός αριθμός και R ένας μεταθετικός μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, τότε **η ορίζουσα** $\det(\mathbf{A})$ ενός πίνακα

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

ορίζεται μέσω τού τύπου τού Leibniz:

$$\boxed{\det(\mathbf{A}) := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma)\, a_{1\,\sigma(1)}\, a_{2\,\sigma(2)} \cdots a_{n\,\sigma(n)}} \tag{1.20}$$

με το άθροισμα εκτεινόμενο υπεράνω όλων των μετατάξεων σ τού συνόλου $\{1, 2, \ldots, n\}$, και

$$\mathrm{sgn}(\sigma) := \prod_{1\leq i<j\leq n} \tfrac{\sigma(j)-\sigma(i)}{j-i} \in \{\pm 1\}.$$

Να αποδειχθούν τα ακόλουθα:

(i) Για κάθε $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ισχύει η ισότητα $\det(\mathbf{A}^\intercal) = \det(\mathbf{A})$, όπου $\mathbf{A}^\intercal$ είναι ο **ανάστροφος**[27] τού πίνακα $\mathbf{A}$.

(ii) Εάν όλες οι εγγραφές κάποιας γραμμής (και αντιστοίχως, κάποιας στήλης) ενός πίνακα $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$ είναι ίσες με 0_R, τότε $\det(\mathbf{A}) = 0_R$.

(iii) Εάν $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$ ($n \geq 2$) με $\Sigma\tau_i(\mathbf{A}) = \Sigma\tau_j(\mathbf{A})$ (και αντιστοίχως, με $\Gamma\varrho_i(\mathbf{A}) = \Gamma\varrho_j(\mathbf{A})$) για κάποιους $i, j \in \{1, \ldots, n\}$, $i < j$, τότε $\det(\mathbf{A}) = 0_R$.

(iv) Εάν $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$, $\mathbf{b} = (b_1, \ldots, b_n) \in \mathrm{Mat}_{1\times n}(R)$, και $r, r' \in R$, τότε

$$\det\begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ r\Gamma\varrho_k(\mathbf{A}) + r'\mathbf{b} \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = r\det(\mathbf{A}) + r'\det\begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \mathbf{b} \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix}$$

και

$$\begin{aligned} &\det\left(\Sigma\tau_1(\mathbf{A}) \,\cdots\, \Sigma\tau_{k-1}(\mathbf{A})\, (r\Sigma\tau_k(\mathbf{A}) + r'\mathbf{b}^\intercal)\, \Sigma\tau_{k+1}(\mathbf{A}) \,\cdots\, \Sigma\tau_n(\mathbf{A})\right) \\ &= r\det(\mathbf{A}) + r'\det\left(\Sigma\tau_1(\mathbf{A}) \,\cdots\, \Sigma\tau_{k-1}(\mathbf{A})\, \mathbf{b}^\intercal\, \Sigma\tau_{k+1}(\mathbf{A}) \,\cdots\, \Sigma\tau_n(\mathbf{A})\right) \end{aligned}$$

για κάθε[28] $k \in \{1, ..., n\}$.

[27] Οι εγγραφές τού $\mathbf{A}^\intercal$ αποκτώνται ύστερα από *κατοπτρισμό* των εγγραφών τού $\mathbf{A}$ ως προς την κυρία διαγώνιό του. Σημειωτέον ότι $(\mathbf{A}^\intercal)^\intercal = \mathbf{A}$ και $(r\mathbf{A})^\intercal = r(\mathbf{A}^\intercal)$ για κάθε $r \in R$. Επιπροσθέτως, $(\mathbf{A}+\mathbf{B})^\intercal = \mathbf{A}^\intercal + \mathbf{B}^\intercal$ και $(\mathbf{AB})^\intercal = \mathbf{B}^\intercal\mathbf{A}^\intercal$ για οιουσδήποτε $\mathbf{A}, \mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$.

[28] Όταν $k = 1$ (και αντιστοίχως, όταν $k = n$), η ειδικής φύσεως γραμμή (στήλη) τοποθετείται στην πρώτη (και αντιστοίχως, στην n-οστή) θέση και οι γραμμές (στήλες) με δείκτες 1 έως $k-1$ (και αντιστοίχως, με δείκτες $k+1$ έως n) παραλείπονται.

(v) Για κάθε $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ισχύουν τα εξής:

(a) Εάν $n \geq 2$ και $k, l \in \{1, ..., n\}$ με $k \neq l$, τότε

$$\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ \Gamma\varrho_k(\mathbf{A}) + r\Gamma\varrho_l(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = \det(\mathbf{A}), \quad \forall r \in R.$$

(b) Εάν $k \in \{1, ..., n\}$ και $r \in R$, τότε

$$\det \begin{pmatrix} \Gamma\varrho_1(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_{k-1}(\mathbf{A}) \\ r\Gamma\varrho_k(\mathbf{A}) \\ \Gamma\varrho_{k+1}(\mathbf{A}) \\ \vdots \\ \Gamma\varrho_n(\mathbf{A}) \end{pmatrix} = r \det(\mathbf{A}).$$

(c) Εάν $n \geq 2$, $r \in R$ και $k, l \in \{1, ..., n\}$ με $k \neq l$, τότε

$$\det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{k-1}(\mathbf{A}) \left(\Sigma\tau_k(\mathbf{A}) + r\Sigma\tau_l(\mathbf{A})\right) \Sigma\tau_{k+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right) = \det(\mathbf{A}).$$

(d) Εάν $k \in \{1, ..., n\}$ και $r \in R$, τότε

$$\det\left(\Sigma\tau_1(\mathbf{A}) \ \cdots \ \Sigma\tau_{k-1}(\mathbf{A}) \left(r\Sigma\tau_k(\mathbf{A})\right) \Sigma\tau_{k+1}(\mathbf{A}) \ \cdots \ \Sigma\tau_n(\mathbf{A})\right) = r \det(\mathbf{A}).$$

(e) Για κάθε $r \in R$ ισχύει η ισότητα $\det(r\mathbf{A}) = r^n \det(\mathbf{A})$.

(f) Για κάθε $\tau \in \mathfrak{S}_n$ ισχύουν οι ισότητες

$$\det \begin{pmatrix} \Gamma\varrho_{\tau(1)}(\mathbf{A}) \\ \vdots \\ \vdots \\ \Gamma\varrho_{\tau(n)}(\mathbf{A}) \end{pmatrix} = \det\left(\Sigma\tau_{\tau(1)}(\mathbf{A}) \ \cdots \ \Sigma\tau_{\tau(n)}(\mathbf{A})\right) = \mathrm{sgn}(\tau) \det(\mathbf{A}).$$

(g) Εάν $a_{ij} = 0_R$ για $i > j$ (και αντιστοίχως, για $i < j$), τότε $\det(\mathbf{A}) = \prod_{i=1}^{n} a_{ii}$. Ιδιαιτέρως, $\det(\mathbf{I}_n) = 1_R$.

(vi) Το γινόμενο των οριζουσών δυο πινάκων $\mathbf{A}, \mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$ ισούται με την ορίζουσα τού γινομένου τους, ήτοι ισχύει η ισότητα[29]

$$\boxed{\det(\mathbf{A}) \det(\mathbf{B}) = \det(\mathbf{AB}).} \tag{1.21}$$

[29] Ως εκ τούτου, $\det(\mathbf{AB}) = \det(\mathbf{BA})$.

(vii) Εάν $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$, όπου $n > 1$, τότε για $i, j \in \mathbb{N}$ με $1 \leq i, j \leq n$, ορίζουμε τον «ελάσσονα πίνακα»

$$\mathbf{A}^{\sharp}_{[i,j]} := \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1\,j-1} & a_{1\,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1\,1} & \cdots & a_{i-1\,j-1} & a_{i-1\,j+1} & \cdots & a_{i-1\,n} \\ \hline a_{i+1\,1} & \cdots & a_{i+1\,j-1} & a_{i+1\,j+1} & \cdots & a_{i+1\,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n\,j-1} & a_{n\,j+1} & \cdots & a_{nn} \end{array}\right)$$

τον σχηματιζόμενο από τον $\mathbf{A}$ ύστερα από τη διαγραφή τής i-οστής του γραμμής και τής j-οστής του στήλης. Το στοιχείο

$$\mathrm{cof}_{ij}(\mathbf{A}) := (-1)^{i+j} \det(\mathbf{A}^{\sharp}_{[i,j]}) \tag{1.22}$$

τού R ονομάζεται **συμπαράγοντας** (ή **αλγεβρικό συμπλήρωμα**) τού $\mathbf{A}$ στη θέση (i, j) και ο

$$\boxed{\mathbf{adj}(\mathbf{A}) := (\mathrm{cof}_{ij}(\mathbf{A}))^{\intercal}_{1\leq i,j\leq n}}$$

ο πίνακας ο προσαρτημένος στον $\mathbf{A}$. Η ορίζουσα τού $\mathbf{A}$ εκφράζεται ως ακολούθως:

$$\boxed{\det(\mathbf{A}) = \sum_{k=1}^{n} a_{ik}\,\mathrm{cof}_{ik}(\mathbf{A}) = \sum_{k=1}^{n} (-1)^{i+k}\, a_{ik} \det(\mathbf{A}^{\sharp}_{[i,k]}).}$$

(Αυτός ο τύπος λέγεται *τύπος αναπτύγματος τής* $\det(\mathbf{A})$ *ως προς την* i*-οστή γραμμή*.) Κατ' αναλογίαν,

$$\boxed{\det(\mathbf{A}) = \sum_{k=1}^{n} a_{kj}\,\mathrm{cof}_{kj}(\mathbf{A}) = \sum_{k=1}^{n} (-1)^{k+j}\, a_{kj} \det(\mathbf{A}^{\sharp}_{[k,j]}).}$$

(*Τύπος αναπτύγματος τής* $\det(\mathbf{A})$ *ως προς την* j*-οστή στήλη*.)

(viii) Για οιονδήποτε φυσικό αριθμό n και για οιονδήποτε $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ισχύουν οι ισότητες

$$\boxed{\det(\mathbf{A})\ \mathbf{I}_n = \mathbf{A}\,\mathbf{adj}(\mathbf{A}) = \mathbf{adj}(\mathbf{A})\ \mathbf{A}.} \tag{1.23}$$

1-20. Έστω R ένας δακτύλιος. Ως **κέντρο** τού R ορίζεται το σύνολο

$$\boxed{Z(R) := \{\, a \in R \mid\ ar = ra,\ \forall r \in R \}\,.}$$

(i) Να αποδειχθεί ότι $Z(R) = R$ εάν και μόνον εάν ο R είναι μεταθετικός.

(ii) Να αποδειχθεί ότι το $Z(R)$ αποτελεί έναν υποδακτύλιο τού R.

(iii) Εάν ο R έχει μοναδιαίο στοιχείο, τότε το ίδιο ισχύει και για τον $Z(R)$ και μάλιστα $1_{Z(R)} = 1_R$.

(iv) Εάν $n \in \mathbb{N}$ και εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, ποιο είναι το κέντρο $Z(\mathrm{Mat}_{n\times n}(R))$ τού δακτυλίου $\mathrm{Mat}_{n\times n}(R)$;

(v) Εάν ο R είναι διαιρετικός δακτύλιος, να αποδειχθεί ότι το $Z(R)$ είναι σώμα.

(vi) Ποιο είναι το κέντρο $Z(\mathbb{H}_{\mathbb{R}})$ τού διαιρετικού δακτυλίου $\mathbb{H}_{\mathbb{R}}$ των τετρανίων;

(vii) Να αποδειχθεί ότι το $\{a\mathbf{I} + b\mathbf{i} \mid a, b \in \mathbb{R}\}$ είναι ένας υποδακτύλιος τού $\mathbb{H}_{\mathbb{R}}$ που αποτελεί ένα σώμα μη περιεχόμενο εντός τού $Z(\mathbb{H}_{\mathbb{R}})$.

1-21. Έστω R ένας δακτύλιος για τον οποίο ισχύει $r^2 - r \in Z(R)$ για κάθε $r \in R$. Να αποδειχθεί ότι ο R είναι μεταθετικός.

1-22. Εάν τα R και S είναι δυο ακέραιες περιοχές (και, αντιστοίχως, δυο σώματα), είναι και το καρτεσιανό τους γινόμενο $R \times S$ (με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού, βλ. 1.1.4 (v)) ακεραία περιοχή (και, αντιστοίχως, σώμα);

1-23. Για οιοδήποτε $\varepsilon \in \mathbb{R}_{>0}$ ορίζουμε το $U_\varepsilon := \{\xi \mid \xi \in \mathbb{R},\ |\xi| < \varepsilon\}$, καθώς και τα σύνολα

$$\begin{cases} \mathcal{C}^n(U_\varepsilon) := \left\{ f \in \mathbb{R}^{U_\varepsilon} \;\middle|\; f \ \ n \text{ φορές συνεχώς παραγωγίσιμη} \right\}, \forall n \in \mathbb{N}, \\ \mathcal{C}^\infty(U_\varepsilon) := \left\{ f \in \mathbb{R}^{U_\varepsilon} \;\middle|\; f \text{ απειράκις παραγωγίσιμη} \right\}, \\ \mathcal{C}^\omega(U_\varepsilon) := \left\{ f \in \mathbb{R}^{U_\varepsilon} \;\middle|\; \begin{array}{l} f \text{ αναπαραστάσιμη ως δυναμοσειρά} \\ \text{περί το } 0 \text{ με ακτίνα συγκλίσεως } \geq \varepsilon \end{array} \right\}. \end{cases}$$

Να αποδειχθεί ότι κάθε μέλος τής ακολουθίας διαδοχικώς εγκλειομένων συνόλων

$$\mathcal{C}^\omega(U_\varepsilon) \subsetneqq \mathcal{C}^\infty(U_\varepsilon) \subsetneqq \cdots \subsetneqq \mathcal{C}^n(U_\varepsilon) \subsetneqq \mathcal{C}^{n-1}(U_\varepsilon) \subsetneqq \cdots \subsetneqq \mathcal{C}^1(U_\varepsilon) \subsetneqq \mathbb{R}^{U_\varepsilon}$$

είναι υποδακτύλιος τού επομένου του (εξ αριστερών προς τα δεξιά). Εν συνεχεία, να αποδειχθεί ότι ο $\mathcal{C}^\omega(U_\varepsilon)$ δεν έχει μηδενοδιαιρέτες, ενώ όλοι οι υπόλοιποι έχουν.

1-24. Έστω S ένας υποδακτύλιος ενός δακτυλίου R. Εάν αμφότεροι οι S και R διαθέτουν μοναδιαίο στοιχείο και $1_S \neq 1_R$, να αποδειχθεί ότι το 1_S είναι ένας μηδενοδιαιρέτης εντός τού R.

1-25. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Να αποδειχθούν τα ακόλουθα:

(i) Εάν $a, b \in R$ και $ab = ba$, τότε

$$a^m b^n = b^n a^m, \ \ (ab)^n = a^n b^n,$$

για κάθε ζεύγος $(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0$.

(ii) Εάν $a, b \in R^\times$ και $ab = ba$, τότε $a^m b^n = b^n a^m$, $(ab)^n = a^n b^n$, για κάθε ζεύγος $(m,n) \in \mathbb{Z} \times \mathbb{Z}$. (Βλ. 1.2.9).

(iii) $(a^{-1})^n = (a^n)^{-1}$, $a^n = \left(a^{-1}\right)^{-n}$, $\forall a \in R^\times$ και $\forall n \in \mathbb{Z}$. (Βλ. 1.2.9).

1-26. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Υποθέτοντας την ύπαρξη δύο στοιχείων $a, b \in R$, για τα οποία ισχύουν οι ισότητες

$$ab + ba = 1_R, \;\; a^2 b + b a^2 = a,$$

να αποδειχθεί ότι $a \in R^\times$ με το $2b$ ως αντίστροφό του.

1-27. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Υποθέτοντας ότι τα στοιχεία $x, y \in R$ είναι δεξιά αντίστροφα ενός $u \in R$ (ήτοι ότι $ux = uy = 1_R$), να αποδειχθεί (i) ότι *και* το $xu + y - 1_R$ είναι δεξιό αντίστροφο τού u, και (ii) ότι το u διαθέτει *άπειρα* δεξιά αντίστροφα όταν $x \neq y$.

1-28. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το $a \in R$ είναι ένα μηδενοδύναμο στοιχείο τού R, να αποδειχθεί ότι το $1_R + a$ είναι αντιστρέψιμο.

1-29. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω τυχόν $x \in R$. Να αποδειχθούν τα ακόλουθα:

(i) Το $1_R - x$ είναι αντιστρέψιμο με αντίστροφό του το $1_R + y \Leftrightarrow \exists y \in R : y - x = xy = yx$.

(ii) Για οιοδήποτε $y \in R$, το $1_R - xy$ είναι αντιστρέψιμο $\Longleftrightarrow$ το $1_R - yx$ είναι αντιστρέψιμο.

(iii) Το $1_R - xy$ είναι αντιστρέψιμο για κάθε $y \in R \Longleftrightarrow$ το $1_R - zxy$ είναι αντιστρέψιμο για οιαδήποτε $y, z \in R$.

1-30. Εάν $n \in \mathbb{N}$ και οι $R_1, \ldots, R_n$ είναι μη τετριμμένοι δακτύλιοι με μοναδιαίο στοιχείο, να αποδειχθεί ότι $(R_1 \times \cdots \times R_n)^\times = R_1^\times \times \cdots \times R_n^\times$.

1-31. Έστω το σύνολο $R := \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$ εφοδιασμένο με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ρητών αριθμών. Να αποδειχθούν τα ακόλουθα:

(i) Το R είναι δακτύλιος και $\mathbb{Z} \subsetneqq R \subsetneqq \mathbb{Q}$,

(ii) Το R είναι ακεραία περιοχή.

(iii) $R^\times = \{\pm\, 2^\nu \mid \nu \in \mathbb{Z}\}$.

1-32. Έστω

$$R := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \;\middle|\; c = 0 \right\}.$$

(i) Να αποδειχθεί ότι το R είναι υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ με μοναδιαίο στοιχείο του το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{Z})}$.

(ii) Να δειχθεί ότι ο δακτύλιος R δεν είναι μεταθετικός.

(iii) Να προσδιορισθεί η ομάδα $R^\times$.

1-33. Έστω m ένας φυσικός αριθμός ≥ 2 και έστω

$$R := \left\{ \begin{pmatrix} [a]_m & [b]_m \\ [c]_m & [d]_m \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}_m) \;\middle|\; [c]_m = [0]_m \right\}.$$

Να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο R είναι υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$ με μοναδιαίο στοιχείο του το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)}$.

(ii) Ο R δεν είναι μεταθετικός.

(iii) Ισχύει η αμφίπλευρη συνεπαγωγή

$$\begin{pmatrix} [a]_m & [b]_m \\ [0]_m & [d]_m \end{pmatrix} \in R^\times \iff \left([a]_m \in \mathbb{Z}_m^\times \text{ και } [d]_m \in \mathbb{Z}_m^\times \right).$$

(iv) $|R^\times| = m\,\phi(m)^2$, όπου ϕ η συνάρτηση φι τού Euler.

(v) Εάν $m = 2$, τότε η πολλαπλασιαστική ομάδα $(R^\times, \cdot)$ είναι ισόμορφη με την $(\mathbb{Z}_2, +)$.

1-34. Ένα στοιχείο a ενός δακτυλίου R καλείται **ταυτοδύναμο** όταν $a^2 = a$. (Το σύνολο όλων των ταυτοδύναμων στοιχείων τού R σημειώνεται ως $\mathrm{Idem}(R)$.) Να αποδειχθούν τα ακόλουθα:

(i) Έστω R τυχών δακτύλιος. Κάθε $a \in \mathrm{Idem}(R)\setminus\{0_R\}$ είναι μη μηδενοδύναμο.

(ii) Εάν ο R είναι μια ακεραία περιοχή, τότε $\mathrm{Idem}(R)\setminus\{0_R\} = \{1_R\}$.

(iii) Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο και $a, b \in \mathrm{Idem}(R)$, τότε $a + b \in \mathrm{Idem}(R)$ εάν και μόνον εάν $ab = ba$ και $2ab = 0_R$.

(iv) Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο και $a, b \in \mathrm{Idem}(R)$, τότε $a - b \in \mathrm{Idem}(R)$ εάν και μόνον εάν $ab = ba$ και $2(1_R - a)b = 0_R$.

(v) Εάν δυο ταυτοδύναμα στοιχεία a, b ενός δακτυλίου R με μοναδιαίο στοιχείο μετατίθενται αμοιβαίως, ήτοι $ab = ba$, τότε τα

$$ab, \quad a + b - ab, \quad (a - b)^2 = a + b - 2ab$$

είναι ταυτοδύναμα.

1-35. Έστω R ένας μη τετριμμένος δακτύλιος για τον οποίο ισχύει η συνεπαγωγή:

$$[\text{Για κάθε } x \in R \text{ με } x^2 = 0_R \Rightarrow x = 0_R].$$

Να αποδειχθεί ότι κάθε ταυτοδύναμο στοιχείο του ανήκει στο κέντρο του.

1-36. Εάν $m \in \mathbb{N}$, $m \geq 2$, να προσδιορισθεί

(i) το σύνολο $\mathrm{Nil}(\mathbb{Z}_m)$ των μηδενοδύναμων στοιχείων τού $\mathbb{Z}_m$ και

(ii) το σύνολο $\mathrm{Idem}(\mathbb{Z}_m)$ των ταυτοδύναμων στοιχείων τού $\mathbb{Z}_m$.

1-37. Είναι ο δακτύλιος $\mathcal{C}([0,1]) := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f \text{ συνεχής} \right\}$ (ως προς τις πράξεις τής κατά σημείο προσθέσεως και πολλαπλασιασμού) ακεραία περιοχή; Ποια είναι τα σύνολα $\mathrm{Nil}(\mathcal{C}([0,1]))$ και $\mathrm{Idem}(\mathcal{C}([0,1]))$; Ποια είναι η ομάδα $\mathcal{C}([0,1])^{\times}$;

1-38. Έστω R ένας δακτύλιος. Εάν ο R είναι μεταθετικός, να αποδειχθεί ότι το άθροισμα δύο μηδενοδύναμων στοιχείων του είναι μηδενοδύναμο. Εν συνεχεία, να προσδιορισθούν δύο μηδενοδύναμα στοιχεία τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$, το άθροισμα των οποίων δεν είναι μηδενοδύναμο.

1-39. Έστω R ένας μη τετριμμένος δακτύλιος. Υποτιθεμένου ότι η «εξίσωση»

$$ax = b$$

είναι επιλύσιμη για οιαδήποτε $a, b \in R \smallsetminus \{0_R\}$, να αποδειχθεί ότι ο R είναι στρεβλό σώμα.

1-40. Να αποδειχθεί ότι σε κάθε στρεβλό σώμα R ισχύει η ισότητα

$$aba = a - \left(a^{-1} + \left(b^{-1} - a\right)^{-1}\right)^{-1},$$

για οιαδήποτε $a, b \in R \smallsetminus \{0_R\}$ με $a \neq b^{-1}$.

1-41. Έστω R ένας δακτύλιος με τουλάχιστον δύο στοιχεία. Υποθέτοντας ότι για κάθε $a \in R \smallsetminus \{0_R\}$ υπάρχει ένα *μονοσημάντως ορισμένο* $b \in R$, τέτοιο ώστε να ισχύει $aba = a$, να αποδειχθούν τα ακόλουθα:

(i) Ο R δεν διαθέτει μηδενοδιαιρέτες.

(ii) $bab = b$, $\forall a \in R \smallsetminus \{0_R\}$.

(iii) Ο R έχει μοναδιαίο (πολλαπλασιαστικό) στοιχείο.

(iv) Ο R είναι στρεβλό σώμα.

1-42. Εάν το K είναι ένα σώμα και το L ένα υποσύνολό του που περιέχει τουλάχιστον δύο στοιχεία, να αποδειχθεί ότι το L είναι υπόσωμα τού K εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:

(i) $1_K \in L$ και $a - b \in L$, για οιαδήποτε $a, b \in L$,

(ii) $ab^{-1} \in L$, για κάθε $a \in L$ και κάθε $b \in L \smallsetminus \{0_K\}$.

Εν συνεχεία, να αποδειχθεί ότι η τομή των μελών οιασδήποτε μη κενής οικογενείας υποσωμάτων $(L_j)_{j \in J}$ ενός σώματος K είναι ένα υπόσωμα τού K.

1-43. Να αποδειχθεί λεπτομερώς ότι ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. 1.1.11 (ii)) είναι ακεραία περιοχή αλλά όχι και σώμα.

1-44. Για οιονδήποτε ακέραιο m ο οποίος δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{|m|} \notin \mathbb{Q}$), να αποδειχθούν τα ακόλουθα:

(i) Για οιαδήποτε στοιχεία $a + b\sqrt{m}$ και $c + d\sqrt{m}$ τού δακτυλίου $\mathbb{Z}[\sqrt{m}]$ (βλ. (1.9)) ισχύει η αμφίπλευρη συνεπαγωγή

$$a + b\sqrt{m} = c + d\sqrt{m} \Longleftrightarrow a = c \text{ και } b = d.$$

(ii) Ο δακτύλιος $\mathbb{Z}[\sqrt{m}]$ (βλ. (1.9)) είναι *ακεραία περιοχή*.

(iii) Για κάθε $r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ (βλ. (1.14)) ισχύει η αμφίπλευρη συνεπαγωγή $r^2 - ms^2 = 0 \Longleftrightarrow r = s = 0$.

(iv) Ο δακτύλιος $\mathbb{Q}[\sqrt{m}]$ είναι *υπόσωμα* τού $\mathbb{C}$, οπότε $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m})$.

(v) Επειδή ο m γράφεται ως γινόμενο $m = m'k$ δύο μονοσημάντως ορισμένων ακεραίων m' και $k \geq 1$, όπου ο μεν m' στερείται τετραγώνων[30], ο δε k είναι τέλειο τετράγωνο, ισχύουν οι ισότητες

$$\mathbb{Z}[\sqrt{m}] = \mathbb{Z}[\sqrt{m'}] \text{ και } \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m'}).$$

(Γι' αυτόν τον λόγο είθισται στον ορισμό αυτών να υποθέτουμε εξαρχής ότι το υπόρριζο m *στερείται τετραγώνων*. Εν τοιαύτη περιπτώσει, λέμε ότι ο $\mathbb{Z}[\sqrt{m}]$ είναι η **τετραγωνική αριθμητική περιοχή** η αντιστοιχιζόμενη στον m και, κατ' αναλογίαν, ότι το σώμα $\mathbb{Q}(\sqrt{m})$ είναι το **τετραγωνικό αριθμητικό σώμα** το αντιστοιχιζόμενο στον m.)

(vi) Εάν οι m_1, m_2 είναι ακέραιοι που στερούνται τετραγώνων, τότε

$$[\mathbb{Z}[\sqrt{m_1}] = \mathbb{Z}[\sqrt{m_2}] \Leftrightarrow m_1 = m_2]$$

και $[\mathbb{Q}(\sqrt{m_1}) = \mathbb{Q}(\sqrt{m_2}) \Leftrightarrow m_1 = m_2]$.

1-45. Να εξετασθεί εάν τα σύνολα $A := \{\, a + b\sqrt[3]{2} \;\big|\; a, b \in \mathbb{Q}\}$ και

$$B := \{\, a + b\sqrt[3]{3} + c\sqrt[3]{9} \;\Big|\; a, b, c \in \mathbb{Q}\}$$

αποτελούν υποσώματα τού σώματος $\mathbb{R}$ των πραγματικών αριθμών.

1-46. (i) Εάν

$$R := \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \;\Big|\; a, b \in \mathbb{Q} \right\},$$

[30] Λέμε ότι ένας ακέραιος αριθμός d **στερείται τετραγώνων** όταν $d \in \mathbb{Z} \smallsetminus \{0, 1\}$ και $\nexists c \in \mathbb{N}, c \geq 2$, τέτοιο ώστε να ισχύει $c^2 \mid d$. Αυτό σημαίνει ότι είτε $d = -1$ είτε $|d| = p_1 \cdots p_k$, όπου $k \in \mathbb{N}$ και οι $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί (*σαφώς διακεκριμένοι* όταν $k \geq 2$), δηλαδή ότι $d \in \{-1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11, \pm 13, \ldots\}$.

να αποδειχθεί ότι το R είναι μεταθετικός υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{Q})$ με μοναδιαίο στοιχείο του το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{Q})}$ και, επιπροσθέτως, σώμα.

(ii) Εάν

$$R_k := \left\{ \begin{pmatrix} x & y \\ -ky & x+2y \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \;\middle|\; x, y \in \mathbb{R} \right\},\ k \in \mathbb{R},$$

να αποδειχθεί ότι το R_k είναι μεταθετικός υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ με μοναδιαίο στοιχείο το $1_{\mathrm{Mat}_{2\times 2}(\mathbb{R})}$, για κάθε $k \in \mathbb{R}$, και να προσδιορισθούν οι τιμές τού k για τις οποίες ο R_k είναι σώμα.

1-47. Να αποδειχθεί η ύπαρξη σώματος με 4 στοιχεία.

1-48. Έστω R ένας μη τετριμμένος πεπερασμένος μεταθετικός δακτύλιος χωρίς μηδενοδιαιρέτες. Να αποδειχθούν τα ακόλουθα:

(i) Ο R έχει μοναδιαίο στοιχείο.

(ii) Ο R είναι σώμα.

1-49. Εάν $n \in \mathbb{N}$, πόσα (σαφώς διακεκριμένα) πολυώνυμα βαθμού $\leq n$ περιέχονται εντός τού δακτυλίου $\mathbb{Z}_2[\mathsf{X}]$;

1-50. Να αποδειχθεί ότι ο σταθερός όρος οιουδήποτε πολυωνύμου $\varphi(\mathsf{X}) \in \mathbb{Z}_4[\mathsf{X}]^\times$ ισούται είτε με το $[1]_4$ είτε με το $[3]_4$. Εν συνεχεία, να αποδειχθεί ότι μεταξύ των αντιστρεψίμων στοιχείων τού δακτυλίου $\mathbb{Z}_4[\mathsf{X}]$ συγκαταλέγονται και (απειροπληθή) πολυώνυμα θετικού βαθμού.

1-51. Έστω K ένα σώμα. Να αποδειχθεί ότι οι ακέραιες περιοχές $K[\mathsf{X}]$ και $K[\![\mathsf{X}]\!]$ δεν είναι σώματα.

1-52. Δοθέντος ενός μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θεωρούμε το σύνολο $R^{\mathbb{Z}}$ όλων των ακολουθιών

$$(\ldots\ldots, a_{-3}, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots\ldots),\ \ a_i \in R,\ \ \forall i \in \mathbb{Z},$$

καθώς και το υποσύνολο $\mathfrak{L}$ τού $R^{\mathbb{Z}}$ το απαρτιζόμενο από εκείνες τις ακολουθίες για τις οποίες υπάρχουν *το πολύ πεπερασμένου πλήθους* $a_i,\ i<0$, που είναι $\neq 0_R$. Επί τού $R^{\mathbb{Z}}$ ορίζονται πράξεις *προσθέσεως* και *πολλαπλασιασμού* ως ακολούθως:

$$(.., a_{-1}, a_0, a_1, ..) + (.., b_{-1}, b_0, b_1, ..) := (\ldots, a_{-1}+b_{-1}, a_0+b_0, a_1+b_1, \ldots),$$

$$(\ldots, a_{-1}, a_0, a_1, \ldots) \cdot (\ldots, b_{-1}, b_0, b_1, \ldots) := (\ldots, c_{-1}, c_0, c_1, \ldots),$$

όπου $c_m := \sum_{(i,j)\in\mathbb{Z}\times\mathbb{Z}:\, i+j=m} a_i b_j,\ \forall m \in \mathbb{Z}$ (με το πλήθος των μη μηδενικών προσθετέων τού c_m *το πολύ πεπερασμένο*[31]). Να αποδειχθούν τα ακόλουθα:

[31] Επειδή (εξ υποθέσεως) καθένα εκ των συνόλων $\{\, i \in \mathbb{Z} |\, i < 0 \text{ και } a_i \neq 0_R\}$ και $\{\, j \in \mathbb{Z} |\, j < 0 \text{ και } b_j \neq 0_R\}$ είναι είτε κενό είτε πεπερασμένο, το σύνολο $\{\, (i,j) \in \mathbb{Z}\times\mathbb{Z} |\, i+j = m \text{ και } a_i b_j \neq 0_R\}$ οφείλει να είναι το πολύ πεπερασμένο *για κάθε* $m \in \mathbb{Z}$.

(i) Η τριάδα $(R^{\mathbb{Z}}, +, \cdot)$ αποτελεί έναν δακτύλιο με μηδενικό του στοιχείο το $(..., 0_R, 0_R, 0_R, 0_R, 0_R, \dots)$ και μοναδιαίο του στοιχείο το $(..., 0_R, \underbrace{1_R}_{\text{θέση με δείκτη } 0}, 0_R, \dots)$ και η τριάδα $(\mathfrak{L}, +, \cdot)$ έναν υποδακτύλιο τού $(R^{\mathbb{Z}}, +, \cdot)$ (με το ίδιο μοναδιαίο στοιχείο). Εάν

$$\mathsf{X} := (..., 0_R, \underbrace{0_R}_{\text{θέση με δείκτη } 0}, \underbrace{1_R}_{\text{θέση με δείκτη } 1}, 0_R, 0_R, \dots),$$

τότε, βάσει των ως άνω πράξεων, κάθε στοιχείο

$$(\dots\dots, 0_R, 0_R, a_{-n}, \dots, a_{-3}, a_{-2}, a_{-1}, a_0, a_1, a_2, \dots\dots),$$

τού $\mathfrak{L}$ (όπου $a_i = 0_R$ για κάθε ακέραιον $i < -n$) γράφεται υπό τη μορφή

$$a_{-n}\mathsf{X}^{-n} + a_{n-1}\mathsf{X}^{-n+1} + \cdots + a_{-1}\mathsf{X}^{-1} + a_0 + a_1\mathsf{X} + a_2\mathsf{X}^2 + \cdots =: \sum_{i=-n}^{\infty} a_i\mathsf{X}^i.$$

Σημείωση: Ο δακτύλιος $(\mathfrak{L}, +, \cdot)$ συμβολίζεται ως $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ και καλείται **δακτύλιος των επίτυπων σειρών Laurent** μιας **απροσδιορίστου**) X με συντελεστές ειλημμένους από τον R.

(ii) Κάθε στοιχείο τού $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ τής μορφής $\varphi(\mathsf{X}) = \sum_{i=-n}^{\infty} a_i\mathsf{X}^i$ για το οποίο

$$\exists m \in \mathbb{N}_0 : a_i = 0_R \text{ για κάθε ακέραιον } i > m$$

καλείται **επίτυπο πολυώνυμο Laurent** μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Το σύνολο αυτών των πολυωνύμων συμβολίζεται ως $R\left[\mathsf{X}, \mathsf{X}^{-1}\right]$ ή $R[\mathsf{X}^{\pm 1}]$, αποτελεί υποδακτύλιο τού $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ (με το ίδιο μοναδιαίο στοιχείο) και καλείται **δακτύλιος των επίτυπων πολυωνύμων Laurent** μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R.

(iii) Εάν ο R είναι μεταθετικός, τότε και οι $R[\mathsf{X}^{\pm 1}]$ και $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ είναι μεταθετικοί.

(iv) Εάν ο R είναι ακεραία περιοχή, τότε και οι $R[\mathsf{X}^{\pm 1}]$ και $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ είναι ακέραιες περιοχές.

(v) $\mathrm{χαρ}(R) = \mathrm{χαρ}(\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]) = \mathrm{χαρ}(R[\mathsf{X}^{\pm 1}])$.

(vi) Εάν ο R είναι ακεραία περιοχή, τότε ένα στοιχείο $\varphi(\mathsf{X}) \in R[\mathsf{X}^{\pm 1}]$ είναι αντιστρέψιμο εάν και μόνον εάν $\exists a \in R^{\times}$ και $k \in \mathbb{Z} : \varphi(\mathsf{X}) = a\,\mathsf{X}^k$.

(vii) Εάν ο R είναι ακεραία περιοχή, ένα $\varphi(\mathsf{X}) = \sum_{i=-n}^{\infty} a_i\mathsf{X}^i \in \mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ με $a_{-n} \neq 0_R$ ($n \in \mathbb{N}$) είναι αντιστρέψιμο εάν και μόνον εάν $a_{-n} \in R^{\times}$.

(viii) Οι $R[\mathsf{X}]$, $R[\mathsf{X}^{\pm 1}]$ και $R[\![\mathsf{X}]\!]$ δεν είναι ποτέ στρεβλά σώματα ή σώματα.

(ix) Ο δακτύλιος $\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ είναι στρεβλό σώμα (και αντιστοίχως, σώμα) εάν και μόνον εάν ο R είναι στρεβλό σώμα (και αντιστοίχως, σώμα).

1-53. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω S ένας υποδακτύλιος αυτού έχων ως μοναδιαίο του στοιχείο το 1_R. Εάν $\{a_1, ..., a_k\}$ είναι ένα πεπερασμένο υποσύνολο τού R, να αποδειχθεί ότι ο δακτύλιος που προκύπτει ύστερα από προσάρτηση αυτού στον S (βλ. εδ. 1.1.15) είναι ο

$$S[a_1, ..., a_k] = \{\, \varphi(a_1, ..., a_k) \in R |\, \varphi(\mathsf{X}_1, \dots, \mathsf{X}_k) \in S\,[\mathsf{X}_1, \dots, \mathsf{X}_k]\}\,.$$

1-54. (i) Να αποδειχθεί η πρόταση 1.4.8.

(ii) Εάν ο p είναι ένας πρώτος αριθμός, να αποδειχθεί ότι

$$(\varphi(\mathsf{X}))^p = \varphi(\mathsf{X}^p),\ \ \forall \varphi(\mathsf{X}) \in \mathbb{Z}_p\,[\mathsf{X}]\,.$$

1-55. Εάν το K είναι ένα σώμα χαρακτηριστικής $p > 0$ και ο n ένας σταθερός φυσικός αριθμός, να αποδειχθεί ότι το $L := \{\, x \in K \mid x^{p^n} = x\}$ είναι ένα υπόσωμα τού K.

1-56. Να προσδιορισθεί χαρακτηριστική τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$, $m \in \mathbb{N}$, καθώς και η χαρακτηριστική τού διαιρετικού δακτυλίου $\mathbb{H}_{\mathbb{R}}$ των τετρανίων.

1-57. Να αποδειχθεί ότι η χαρακτηριστική οιασδήποτε υποπεριοχής μιας ακεραίας περιοχής R είναι ίση με τη χαρακτηριστική τής R.

1-58. Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, $\chi\alpha\rho(R) \notin \{1, 2\}$ και με την ομάδα $(R^\times, \cdot)$ των αντιστρεψίμων στοιχείων του κυκλική, να αποδειχθεί ότι η $(R^\times, \cdot)$ είναι πεπερασμένη τάξεως $|R^\times| \equiv 0 \,(\mathrm{mod}\, 2)$.

1-59. Εάν τα R και S είναι δυο δακτύλιοι, να αποδειχθούν τα ακόλουθα για τον δακτύλιο $R \times S$ (βλ. 1.1.4 (v)):

(i) Εάν $\chi\alpha\rho(R) = m \in \mathbb{N}$ και $\chi\alpha\rho(R) = n \in \mathbb{N}$, τότε $\chi\alpha\rho(R \times S) = \varepsilon\kappa\pi(m, n)$.

(ii) Εάν ένας τουλάχιστον εκ των R, S έχει χαρακτηριστική ίση με το μηδέν, τότε και ο $R \times S$ έχει χαρακτηριστική ίση με το μηδέν.

1-60. Εάν $n \in \mathbb{N}$, ο p είναι ένας πρώτος αριθμός και ο R ένας δακτύλιος με μοναδιαίο στοιχείο χαρακτηριστικής p^n, να αποδειχθούν τα ακόλουθα:

(i) Εάν $r \in R$, τότε το $1_R - r$ είναι μηδενοδύναμο εάν και μόνον εάν το r είναι αντιστρέψιμο και η τάξη τού r εντός τής $R^\times$ ισούται με μία δύναμη τού p.

(ii) Εάν $\mathrm{Nil}(R) = \{0_R\}$ και εάν το $a \in R^\times$ είναι ένα στοιχείο πεπερασμένης τάξεως, τότε $\mu\kappa\delta(p, \mathrm{ord}(a)) = 1$.

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).)

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

[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.

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* $a\in I$, $r\in R$.

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

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

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

και

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

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

$$\left(\begin{array}{cc} a & b\\ 0 & 0\end{array}\right)-\left(\begin{array}{cc} a' & b'\\ 0 & 0\end{array}\right)=\left(\begin{array}{cc} a-a' & b-b'\\ 0 & 0\end{array}\right)\in I$$

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

$$\left(\begin{array}{cc} a & b\\ 0 & 0\end{array}\right)\left(\begin{array}{cc} c & d\\ e & f\end{array}\right)=\left(\begin{array}{cc} ca+eb & ad+bf\\ 0 & 0\end{array}\right)\in I.$$

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

$$\left(\begin{array}{cc} 1 & 1\\ 1 & 1\end{array}\right)\left(\begin{array}{cc} 1 & 1\\ 0 & 0\end{array}\right)=\left(\begin{array}{cc} 1 & 1\\ 1 & 1\end{array}\right)\notin I.$$

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 $I\subsetneq R$ λέγεται ***γνήσιο*** *(αριστερό/δεξιό/αμφίπλευρο)* **ιδεώδες**.

[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.

(v) Εάν 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

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

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 $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ των μελών της αποτελεί ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού 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

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

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 $a \in I \setminus \{0_R\}$, ούτως ώστε να ισχύει

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

για κάποιο $b \in R \setminus \{0_R\}$, τότε από τον ορισμό ενός (αριστερού/ δεξιού/ αμφιπλεύρου) ιδεώδους είναι πρόδηλο ότι και τα γινόμενα αυτά (που είναι ίσα 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 I ένα αριστερό ιδεώδες αυτού με $\{0_R\} \subsetneqq I$, τότε υπάρχει κάποιο $a \in I \setminus \{0_R\}$. 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 $a \in R \setminus \{0_R\}$ και το αριστερό, μη τετριμμένο ιδεώδες Ra τού R, παρατηρούμε ότι

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

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

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

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 $A \subseteq R$. Λέμε ότι 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, είναι **το ιδεώδες το παραγόμενο από το** A ή το ιδεώδες **με γεννήτορες** τα στοιχεία τού A. Όταν $A = \varnothing$, τότε $\langle A\rangle = \{0_R\}$. Κάθε ιδεώδες τού R που μπορεί να γραφεί υπό τη μορφή $\langle A\rangle$, όπου $A \subseteq R$ είναι κάποιο πεπερασμένο υποσύνολο αυτού, ας πούμε το $A = \{a_1, \ldots, a_k\}$ (όπου $k \in \mathbb{N}$), καλείται **πεπερασμένως παραγόμενο ιδεώδες** και συμβολίζεται απλούστερα ως $\langle a_1, \ldots, a_k\rangle$. Τέλος, κάθε ιδεώδες τού R που μπορεί γραφεί υπό τη μορφή $\langle a\rangle$, για κάποιο $a \in R$, καλείται **κύριο ιδεώδες** (έχον το a ως γεννήτορά του).

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*

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

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

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

όπου κ, μ, ν, ξ είναι θετικοί ακέραιοι αριθμοί.

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

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

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

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

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

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

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

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

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 R ένας δακτύλιος και έστω $a \in R$.*

(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 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 μεταθετικός δακτύλιος, τότε* $\langle a \rangle = \{ r\, a + n\, a \mid r \in R,\ n \in \mathbb{Z} \}$.

(iv) *Εάν ο R είναι 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 $-n$ 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 $a = n_0 q + r$, $q, r \in \mathbb{Z},\ 0 \leq r < n_0$, 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**[3] όταν δεν διαθέτει (αμφίπλευρα) ιδεώδη πέραν τού $\{0_R\}$ και τού R.

2.3.2 Πρόταση. *Κάθε διαιρετικός δακτύλιος είναι απλός.*

ΑΠΟΔΕΙΞΗ. Άμεση συνέπεια τού πορίσματος 2.1.11. □

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 $\mathbf{E}_{ij} \in \mathrm{Mat}_{n\times n}(R)$ ο βοηθητικός πίνακας ο έχων ως εγγραφή του στην i-οστή γραμμή και στην j-οστή στήλη το 1_R και ως λοιπές εγγραφές του το 0_R. Σημειωτέον ότι για οιονδήποτε $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ και οιουσδήποτε δείκτες $i, j \in \{1, ..., n\}$ έχουμε

$$\Gamma\varrho_k(\mathbf{E}_{ij}\mathbf{A}) = \begin{cases} \Gamma\varrho_j(\mathbf{A}), & \text{όταν } k = i, \\ (0_R, ..., 0_R), & \text{όταν } k \in \{1, ..., n\}\setminus\{i\}, \end{cases} \tag{2.2}$$

και

$$\Sigma\tau_k(\mathbf{A}\mathbf{E}_{ij}) = \begin{cases} \Sigma\tau_i(\mathbf{A}), & \text{όταν } k = j, \\ (0_R, ..., 0_R)^{\intercal}, & \text{όταν } k \in \{1, ..., n\}\setminus\{j\}. \end{cases} \tag{2.3}$$

Για την απόδειξη τής προτάσεως θεωρούμε ένα ιδεώδες I 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 υφίστανται $j_0, k_0 \in \{1, ..., n\}$ με $a_{j_0k_0} \neq 0_R$. Για κάθε δείκτη $l \in \{1, ..., n\}$ οι (2.2) και (2.3) μας οδηγούν στο συμπέρασμα ότι[4]

$$\mathbf{E}_{lj_0}\,\mathbf{A}\,\mathbf{E}_{k_0l} = \mathbf{E}_{lj_0}\left(\sum_{i=1}^{n} a_{ik_0}\mathbf{E}_{ik_0}\right) = \sum_{i=1}^{n} a_{ik_0}\mathbf{E}_{lj_0}\mathbf{E}_{ik_0} = a_{j_0k_0}\mathbf{E}_{ll}.$$

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

[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.

Επειδή $\mathbf{A} \in I$ και $\mathbf{E}_{lj_0}, \mathbf{E}_{k_0 l} \in \mathrm{Mat}_{n\times n}(R)$, τούτο σημαίνει ότι $a_{j_0k_0}\mathbf{E}_{ll} \in I$. Επιπροσθέτως, επειδή ο R είναι διαιρετικός δακτύλιος, ορίζεται το αντίστροφο στοιχείο $a^{-1}_{j_0k_0}$ τού $a_{j_0k_0}$. Ως εκ τούτου,

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

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.*

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

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

σχηματίζεται η εξής ακολουθία διαδοχικώς εγκλειομένων κυρίων ιδεωδών:

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

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

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

Όμως τούτο έχει ως συνέπεια ότι $a^n(1_R - ra) = 0_R$, το οποίο, συνδυαζόμενο με το ότι $a^n \in R\setminus\{0_R\}$ 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. □

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 $I_1, \dots, I_n, n \in \mathbb{N}, n \geq 2$, αριστερά (και αντιστοίχως, δεξιά/αμφίπλευρα) ιδεώδη του. Ορίζουμε το **άθροισμα**[5] 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

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

αντιστοίχως[6]. 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 $I_1, \dots, I_n$ 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

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

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 $j \in \{1, \dots, n\}$,

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

[5] Το **άθροισμα** μπορεί να ορισθεί και για *τυχούσες* οικογένειες ιδεωδών $(I_\lambda)_{\lambda \in \Lambda}$ τού R (με $\Lambda \neq \varnothing$) ως ακολούθως:

$$\sum_{\lambda \in \Lambda} I := \left\{ a_{\lambda_1} + \cdots + a_{\lambda_k} \ \middle| \ \begin{array}{c} a_j \in I_j, \ \forall j \in \{\lambda_1, ..., \lambda_k\}, \\ \text{για οιοδήποτε } \{\lambda_1, ..., \lambda_k\} \subseteq \Lambda,\ k \in \mathbb{N} \end{array} \right\}.$$

[6] Προσοχή! Μη συγχέετε το γινόμενο $IJ := \left\{ \sum_{j=1}^{k} a_j b_j \middle| \ a_j \in I, b_j \in J,\ k \in \mathbb{N} \right\}$ δυο ιδεωδών I, J τού R με το σύνολο $\{\, ab |\ a \in I, b \in J\}$! Το τελευταίο ενδέχεται *να μην είναι ιδεώδες* (ακόμη και αν ο R είναι μεταθετικός με μοναδιαίο στοιχείο). Επί παραδείγματι, εάν στον $R = \mathbb{R}[\mathsf{X}_1, \mathsf{X}_2]$ θεωρήσουμε τα $I = J = \langle \mathsf{X}_1, \mathsf{X}_2 \rangle$, τότε τα στοιχεία X_1^2 και X_2^2 ανήκουν στο $\{\, \varphi(\mathsf{X}_1, \mathsf{X}_2)\psi(\mathsf{X}_1, \mathsf{X}_2) |\ \varphi(\mathsf{X}_1, \mathsf{X}_2) \in I,\ \psi(\mathsf{X}_1, \mathsf{X}_2) \in J\}$. Ωστόσο, το άθροισμά τους $\mathsf{X}_1^2 + \mathsf{X}_2^2$ δεν ανήκει σε αυτό.

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[7]. 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 τόσον το 3 όσον 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

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

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 $Rab = \langle ab \rangle$. □

[7] Είναι εύκολο να αποδειχθεί ότι η ένωση $I \cup J$ δυο ιδεωδών I, J ενός δακτυλίου R αποτελεί ιδεώδες αυτού εάν και μόνον εάν είτε $I \subseteq J$ είτε $J \subseteq I$.

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

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

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

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

Όμως, από τον ορισμό τού ιδεώδους,

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

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

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

$$x=\left(\underbrace{\sum_{j=1}^{k}(a_jc_j+a_jd_j+b_jc_j)}_{\in I_1}+\underbrace{\sum_{j=1}^{k}b_jd_j}_{\in I_2\,I_3}\right)\in I_1+I_2\,I_3,$$

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

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

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 $I \subseteq \mathrm{Nil}(R)$.*

ΑΠΟΔΕΙΞΗ. Εάν το I είναι ένα μηδενοδύναμο ιδεώδες ενός δακτυλίου R, τότε υπάρχει $n \in \mathbb{N} : I^n = \{0_R\}$, 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

$$a_n := ([0]_2, [0]_{2^2}, \dots, [0]_{2^{n-1}}, [0]_{2^n}, [2]_{2^{n+1}}, [0]_{2^{n+2}}, [0]_{2^{n+3}}, \dots) \in R$$

(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.*

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

$$a_j^n = 0_R, \ \forall j \in \{1, \dots, \kappa\}. \tag{2.4}$$

Κατά το (iii) τής προτάσεως 2.2.2 υπάρχουν $r_1, \dots, r_\kappa \in R$, 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 (2.4) και τού τύπου (1.6))

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

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

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

Ειδικότερα, για $m = \kappa n$ λαμβάνουμε

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

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

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

Ως εκ τούτου, υπάρχει *τουλάχιστον ένας* δείκτης $\xi \in \{1, \dots, \kappa\}$ με[8] $\lambda_\xi \geq n$, 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

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

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 $m, n \in \mathbb{Z} \setminus \{0\}$, τότε ισχύουν τα εξής*:

(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 $a = \lambda m = \kappa n$, για κάποιους $\lambda, \kappa \in \mathbb{Z}$. Έστω $d := \text{μκδ}(m, n)$. Προφανώς,

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

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

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

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[9]

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

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

[9] Για κάθε $n \in \mathbb{Z}$ θέτουμε $\text{sign}(n) := 1$ όταν $n \geq 0$ και $\text{sign}(n) := -1$ όταν $n < 0$.

όπου $\frac{\mu\,\text{sign}(m)\,|n|}{\mu\kappa\delta(m,n)} \in \mathbb{Z}$ και $\frac{\mu\,\text{sign}(n)\,|m|}{\mu\kappa\delta(m,n)} \in \mathbb{Z}$. Συνεπώς έχουμε $a \in \langle m\rangle \cap \langle n\rangle$, δηλαδή $\langle \epsilon\kappa\pi(m,n)\rangle \subseteq \langle m\rangle \cap \langle n\rangle$.

(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

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

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

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

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

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

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

για κάποιον $c \in \mathbb{Z}$. Άρα

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

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

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

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

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

(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,

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

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 $I_3 \subseteq I_2 + I_3$, συμπεραίνουμε ότι

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

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 $rI_2 + rI_3 = r\,(I_2 + I_3) \subseteq I_1 + I_1 = I_1 \Rightarrow r \in I_1 : (I_2 + I_3)$. Εν συνεχεία, υποθέτουμε ότι $r \in (I_1 \cap I_2) : I_3$, ήτοι ότι ισχύει $rI_3 \subseteq I_1 \cap I_2$. 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 $rI_3 \subseteq I_1 \cap I_2 \Rightarrow r \in (I_1 \cap I_2) : I_3$.
(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

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

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. *Έστω $\mathfrak{p}\subsetneqq R$ ένα ιδεώδες ενός δακτυλίου R. Εάν για οιοδήποτε ζεύγος $(a,b)\in R\times R$ ισχύει η συνεπαγωγή*

$$[ab\in\mathfrak{p}\Longrightarrow \text{είτε } a\in\mathfrak{p} \text{ είτε } b\in\mathfrak{p}], \tag{2.5}$$

τότε το $\mathfrak{p}$ 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 (2.5)*.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε εν πρώτοις ότι η συνθήκη (2.5) ικανοποιείται. Εάν τα I, J είναι ιδεώδη τού R με $IJ\subseteq\mathfrak{p}$ και $I\not\subseteq\mathfrak{p}$, 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 (2.5). □

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

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

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

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

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

(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 (2.5) *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.*

ΑΠΟΔΕΙΞΗ. 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 αποτελεί ένα 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 ισχύει η συνεπαγωγή

$$\left[\left\{ \begin{array}{c} \mathfrak{m} \subseteq \mathfrak{n} \subseteq R \\ \text{για κάποιο ιδεώδες } \mathfrak{n} \text{ τού } R \end{array} \right\} \Longrightarrow \text{είτε } \mathfrak{n} = \mathfrak{m} \ \text{ είτε } \ \mathfrak{n} = R \right].$$

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,

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

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,

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

(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 $a \equiv 1(\mathrm{mod}\,3)$ και $b \equiv 2(\mathrm{mod}\,3)$, τότε

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

Τέταρτη περίπτωση: Εάν $a \equiv 2(\mathrm{mod}\,3)$ και $b \equiv 0(\mathrm{mod}\,3)$, τότε

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

Πέμπτη περίπτωση: Εάν $a \equiv 2(\mathrm{mod}\,3)$ και $b \equiv 1(\mathrm{mod}\,3)$, τότε

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

Έκτη περίπτωση: Εάν $a \equiv 2(\mathrm{mod}\,3)$ και $b \equiv 2(\mathrm{mod}\,3)$, τότε

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

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

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

και $2 + i \in I_5' \setminus I_5$. 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

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

από την οποία θα καταλήγαμε σε άτοπο, αφού θα είχαμε $c, d \in \mathbb{Q} \setminus \mathbb{Z}$.

(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* $\mathfrak{m} + \langle a \rangle = R,\ \forall a \in R \setminus \mathfrak{m}$.

ΑΠΟΔΕΙΞΗ. Έστω $\mathfrak{m} \subsetneqq R$ ένα μεγιστικό ιδεώδες ενός δακτυλίου R. Τότε για κάθε $a \in R \setminus \mathfrak{m}$ 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 $a \in R \setminus \mathfrak{m}$, τότε για οιοδήποτε ιδεώδες $\mathfrak{n}$ τού R, για το οποίο ισχύουν οι εγκλεισμοί $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$, θα υπάρχει κάποιο $b \in \mathfrak{n} \setminus \mathfrak{m}$. Ως εκ τούτου,

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

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

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 $2\mathbb{Z} \setminus \mathfrak{m}$. 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 αυτοπαθής, 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 "$\preceq$". (Επίσης χρησιμοποιείται συχνά και ο συμβολισμός «$\prec$» μεταξύ των στοιχείων τού A, όπου

$x \prec y$ αποτελεί συντομογραφία τού ($x \preceq y$ και $x \neq y$)). Ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ λέγεται **ολικώς (ή γραμμικώς) διατεταγμένο σύνολο** όταν όλα τα στοιχεία τού A είναι μεταξύ τους ανά δύο *συγκρίσιμα*, δηλαδή όταν

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

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 $(\mathbb{Z}, \leq)$, 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

$$A \preceq B \underset{\text{ορσ}}{\iff} A \subseteq B, \ \ \forall\, (A, B) \in \mathfrak{P}(C) \times \mathfrak{P}(C),$$

διαπιστώνουμε ότι το $(\mathfrak{P}(C), \preceq)$ είναι ένα μερικώς διατεταγμένο σύνολο. Σημειωτέον ότι το $(\mathfrak{P}(C), \preceq)$ 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 $(A, \preceq)$ 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 "$\preceq$" όταν $y \preceq x$, $\forall y \in B$.
(ii) Ένα στοιχείο $x \in A$ καλείται **κάτω φράγμα** τού B (εντός τού A) ως προς την "$\preceq$" όταν $x \preceq y$, $\forall y \in B$.

2.5.13 Ορισμός. Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο.
(i) Ένα στοιχείο $x \in A$ καλείται **μεγιστικό (ή μεγιστοτικό) στοιχείο** τού A (ως προς την "$\preceq$") όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $x \preceq y$ 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 "$\preceq$") όταν για κάθε στοιχείο $y \in A$ για το οποίο ισχύει $y \preceq x$ 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 $x \preceq y \underset{\text{ορσ}}{\iff} (y = kx \text{ για κάποιον } k \in \mathbb{Z})$, τότε το ζεύγος $(A, \preceq)$ 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 $(A, \preceq)$ λέγεται **επαγωγικώς διατεταγμένο** όταν κάθε ολικώς διατεταγμένο[10] υποσύνολό του (ως προς την "$\preceq$") διαθέτει ένα άνω φράγμα (εντός τού A).

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[11] (ως προς την "$\subseteq$").

Το ακόλουθο *λήμμα τού Zorn*[12] 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 $(A, \preceq)$ είναι ένα επαγωγικώς διατεταγμένο σύνολο, τότε για οιοδήποτε $a \in A$ υπάρχει τουλάχιστον ένα μεγιστικό στοιχείο m εντός τού A, για το οποίο ισχύει $a \preceq m$.*

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

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,

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

[11] Σημειωτέον ότι *το ίδιο το* $\{B_1, B_2, B_3, ...\}$ έχει το $\bigcup_{k\in\mathbb{N}} B_k \in \mathfrak{P}(A)$ ως άνω φράγμα του.

[12] 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).

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[13]

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

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 $B \neq \varnothing$ τού $\mathcal{S}_R(I)$ και ορίζουμε το σύνολο

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

Προφανώς, $J \subseteq s(B)$ για κάθε $J \in B$. Θα αποδείξουμε ότι $s(B) \in \mathcal{S}_R(I)$ (ήτοι ότι το $s(B)$ είναι *ιδεώδες* τού R με $I \subseteq s(B) \subsetneqq R$). Παρατηρούμε, κατ' αρχάς, ότι $I \subseteq s(B)$ (εξ ορισμού). Εξάλλου, εάν $x, y \in s(B)$, το x ανήκει σε κάποιο $J_x \in B$ και το y σε κάποιο $J_y \in B$. Λόγω τής ολικής διατάξεως τού B 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

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

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

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

Συνεπώς,

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

(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. □

[13] 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).

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 τά 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 $(\mathbb{Q},+,\star)$ και τανάπαλιν. Αρκεί λοιπόν να αποδειχθεί ότι η $(\mathbb{Q},+)$ *στερείται μεγιστικών υποομάδων*[14] (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

$$H\subsetneqq H+\left\langle\frac{r}{s}\right\rangle\subseteq\mathbb{Q}\Rightarrow H+\left\langle\frac{r}{s}\right\rangle=\mathbb{Q},\tag{2.6}$$

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 (2.6) 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.

► **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.*

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

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

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

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). □

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 $\left(I,\ +|_{I\times I}\right)$ αποτελεί μια ορθόθετη προσθετική υποομάδα της. Επομένως υπάρχει μια καλώς ορισμένη ομάδα πηλίκων R/I με πρόσθεση[15]:

$$(a + I) + (b + I) := (a + b) + I\ ,\ \text{ για οιαδήποτε }\ a, b \in R. \tag{2.7}$$

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

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 οιαδήποτε $a, b \in R$ ορίσουμε τον «πολλαπλασιασμό»*:

$$(a + I)\ (b + I) := (ab) + I\ . \tag{2.8}$$

ΑΠΟΔΕΙΞΗ. Η πράξη τού «πολλαπλασιασμού» (2.8) 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 συνάγεται ότι $ab + I = a'b' + I$. Επιπροσθέτως, η εν λόγω πράξη (2.8) 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 (2.7), διότι

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

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

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 $a + I \in \mathrm{Nil}(R/I) \iff \exists n \in \mathbb{N} : a^n \in I$.*

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

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

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

(iv) Εάν $a \in R$, τότε

$$\begin{aligned}a+I \in \mathrm{Nil}(R/I) &\iff \exists n \in \mathbb{N} : (a+I)^n = 0_{R/I} = I\\&\iff \exists n \in \mathbb{N} : a^n + I = I \iff \exists n \in \mathbb{N} : a^n \in I.\end{aligned}$$

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

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

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 συνάγεται 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 $a \in R \setminus \mathfrak{m}$. Επειδή το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R, για οιοδήποτε μη μηδενικό στοιχείο $a + \mathfrak{m}$ τού $R/\mathfrak{m}$ έχουμε

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

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 $a \in \mathfrak{n} \smallsetminus \mathfrak{m}$. Το $a+\mathfrak{m}$ έχει (εξ υποθέσεως) 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 $(2+\mathfrak{m})\,(2+\mathfrak{m}) = 4+\mathfrak{m} = \mathfrak{m} = 0_{2\mathbb{Z}/\mathfrak{m}}$.

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' επέκταση, 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 $K \smallsetminus K^\times = \{0_K\}$ είναι ιδεώδες του.

(ii) Ο δακτύλιος

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

των p-αδικών κλασμάτων (όπου p πρώτος, βλ. άσκηση **1-16**, σελ. 35) είναι τοπικός δακτύλιος, καθότι το (κύριο) ιδεώδες

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

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

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

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 $\mathbb{Z}\smallsetminus\mathbb{Z}^\times = \mathbb{Z}\smallsetminus\{\pm 1\}$ (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. Ο δακτύλιος $K[\mathsf{X}]$ των πολυωνύμων μιας απροσδιορίστου με συντελεστές ειλημμένους από αυτό δεν είναι τοπικός δακτύλιος, διότι το σύνολο

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

(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 απροσδιορίστου 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 $K[\![\mathsf{X}]\!]\smallsetminus K[\![\mathsf{X}]\!]^\times$ 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

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

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

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^ν, *όπου* p *πρώτος αριθμός και* $\nu \in \mathbb{N}$.

ΑΠΟΔΕΙΞΗ. Έστω R τυχών τοπικός δακτύλιος με $\chi\alpha\rho(R) = n > 0$. 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

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

(βλ. προτάσεις 1.4.3 και 1.2.17). Κατ' αναλογίαν, αποδεικνύεται ότι $q \cdot 1_R \in \mathfrak{m}_R$. Επειδή $\mu\kappa\delta(p, q) = 1$, 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^ν, όπου $\nu \in \mathbb{N}$. □

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, αυτά τα δύο σύνολα ταυτίζονται. Σε αυτήν την περίπτωση, το οριζόμενο 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 $X \subseteq X'$, τότε $\mathrm{Ann}_R(X')_\alpha \subseteq \mathrm{Ann}_R(X)_\alpha$ και

$$\mathrm{Ann}_R(X')_\delta \subseteq \mathrm{Ann}_R(X)_\delta.$$

(iv) $X \subseteq \mathrm{Ann}_R(\mathrm{Ann}_R(X)_\alpha)_\delta$ και $X \subseteq \mathrm{Ann}_R(\mathrm{Ann}_R(X)_\delta)_\alpha$.

(v) $\mathrm{Ann}_R(X)_\alpha = \mathrm{Ann}_R(\mathrm{Ann}_R(\mathrm{Ann}_R(X)_\alpha)_\delta)_\alpha$ και

$$\mathrm{Ann}_R(X)_\delta = \mathrm{Ann}_R(\mathrm{Ann}_R(\mathrm{Ann}_R(X)_\delta)_\alpha)_\delta.$$

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

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

(viii) 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. (Ειδική περίπτωση: Όταν ο R είναι μεταθετικός, έχουμε $\mathrm{Ann}_R(I) = \{0_R\} : I$.)

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

(x) Εάν $m \in \mathbb{N}$, $m \geq 2$, και $k \in \mathbb{N} : 1 \leq k < m$ με $k \mid m$, να αποδειχθεί ότι ο μηδενιστής

$$\mathrm{Ann}_{\mathbb{Z}_m}([k]_m) := \{[l]_m \in \mathbb{Z}_m \,|\, l \in \mathbb{Z} : [k]_m[l]_m = [0]_m\}$$

τού μονοσυνόλου $\{[k]_m\}$ εντός τού $\mathbb{Z}_m$ είναι σώμα εάν και μόνον εάν ο k είναι πρώτος αριθμός με $\mathrm{μκδ}(k, \frac{m}{k}) = 1$.

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

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

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

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

και έστω

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

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 (αριστερών/δεξιών/αμφιπλεύρων) 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 $I := \bigcup_{j=1}^{\infty} I_j$ των μελών αυτής αποτελεί ένα (αριστερό/δεξιό/αμφίπλευρο) 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

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

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

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

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

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. Εάν τα I και J είναι δυο ιδεώδη ενός δακτυλίου R, να αποδειχθεί η αμφίπλευρη συνεπαγωγή $I + J = J \Longleftrightarrow I \subseteq J$.

2-10. 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

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

2-11. Να αποδειχθούν τα ακόλουθα:

(i) Εντός τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{-5}]$ 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 τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{2}]$ 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 τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{2}]$ ισχύουν οι ισότητες

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

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

2-12. 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.

2-13. Εάν R_1, R_2 είναι δυο δακτύλιοι με μοναδιαίο στοιχείο, να αποδειχθεί ότι κάθε ιδεώδες τού $R_1 \times R_2$ είναι τής μορφής $I_1 \times I_2$, όπου I_1 είναι ένα ιδεώδες τού R_1 και I_2 ένα ιδεώδες τού R_2.

2-14. Εάν I, J είναι δυο ιδεώδη ενός μεταθετικού δακτυλίου R, να αποδειχθούν τα ακόλουθα:

(i) Εάν $I \subseteq \mathrm{Nil}(R)$ και $J \subseteq \mathrm{Nil}(R)$, τότε $I+J \subseteq \mathrm{Nil}(R)$.

(ii) Εάν αμφότερα τα I, J είναι μηδενοδύναμα ιδεώδη (βλ. εδ. 2.4.8), τότε και το $I+J$ είναι μηδενοδύναμο ιδεώδες τού R.

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

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

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 Φ_α και Φ_δ δεν είναι κατ' ανάγκην επιρριπτικές (ακόμη και όταν ο R έχει μοναδιαίο στοιχείο).

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

(vii) Όταν ο R δεν έχει μοναδιαίο στοιχείο, η Φ δεν είναι κατ' ανάγκην επιρριπτική απεικόνιση.

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 Φ η ορισθείσα στην άσκηση **2-16** *διατηρεί τομές*, *αθροίσματα* και *γινόμενα* ιδεωδών τού R.)

Εν συνεχεία, εάν I είναι ένα ιδεώδες τού R, να αποδειχθεί η αμφίπλευρη συνεπαγωγή:

$$\left[\begin{array}{c}\text{το } I \text{ είναι πρώτο}\\ \text{ιδεώδες τού } R\end{array}\right] \Leftrightarrow \left[\begin{array}{c}\text{το } \mathrm{Mat}_{n\times n}(I) \text{ είναι πρώτο}\\ \text{ιδεώδες τού } \mathrm{Mat}_{n\times n}(R)\end{array}\right].$$

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

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

(iii) Το $\mathrm{SLT}_n(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathbf{LT}_n(R)$.

(iv) Κάθε πίνακας $\mathbf{A} \in \mathbf{SUT}_n(R) \cup \mathbf{SLT}_n(R)$ 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

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

και, κατ' αναλογίαν,

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

2-19. Έστω n ένας φυσικός αριθμός ≥ 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 ≥ 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 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 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 $m = p_1^{\nu_1} \cdots p_k^{\nu_k}$, $k \in \mathbb{N}$, $\nu_1, \ldots, \nu_k \in \mathbb{N}$, είναι η κανονική παράσταση τού m ως γινομένου κατάλληλων δυνάμεων σαφώς διακεκριμένων πρώτων αριθμών $p_1, \ldots, p_k$, να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Nil}(\mathbb{Z}_m) = \{[0]_m\} \Leftrightarrow \nu_1 = \cdots = \nu_k = 1$.

(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 ιδεώδες ενός δακτυλίου R, να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Zdv}(R/I) = \varnothing$ εάν και μόνον εάν για οιαδήποτε $a, b \in R$, για τα οποία ισχύει $ab \in I$, έχουμε είτε $a \in I$ είτε $b \in I$.

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

(iii) 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 $\mathbb{Z}_2[\mathsf{X}]/\left\langle \mathsf{X}^2 + [1]_2\right\rangle$ δεν είναι ακεραία περιοχή. (Ως εκ τούτου, το κύριο ιδεώδες $\left\langle \mathsf{X}^2 + [1]_2\right\rangle$ 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 **1-5**). 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 **1-9**. Να αποδειχθούν τα εξής:

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

(ii) 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 $(\mathfrak{p}_\lambda)_{\lambda\in\Lambda}$ είναι μια **αλυσίδα** πρώτων ιδεωδών τού R, ήτοι μια μη κενή οικογένεια πρώτων ιδεωδών τού R έχουσα την ιδιότητα:

$$[\text{είτε } \mathfrak{p}_{\lambda_1} \subseteq \mathfrak{p}_{\lambda_2} \text{ είτε } \mathfrak{p}_{\lambda_2} \subseteq \mathfrak{p}_{\lambda_1}], \ \ \forall(\lambda_1, \lambda_2) \in \Lambda \times \Lambda,$$

τότε τόσον η ένωση $\bigcup\limits_{\lambda\in\Lambda} \mathfrak{p}_\lambda$ όσον και η τομή $\bigcap\limits_{\lambda\in\Lambda} \mathfrak{p}_\lambda$ των μελών της 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 αποδειχθεί ότι οι ακόλουθες συνθήκες είναι ισοδύναμες:

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

(ii) $I_1 \cap \cdots \cap I_n \subseteq \mathfrak{p}$.

(iii) $I_1 \cdots I_n \subseteq \mathfrak{p}$.

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 $I \subseteq \bigcup\limits_{i=1}^{n} \mathfrak{p}_i$, να αποδειχθεί ότι $\exists\, j \in \{1, \ldots, n\} : I \subseteq \mathfrak{p}_j$.

2-35. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$, $n \geq 2$. Εάν υποτεθεί ότι $\mathfrak{m}_1, ..., \mathfrak{m}_n$ είναι n μεγιστικά ιδεώδη τού R με $\mathfrak{m}_i \neq \mathfrak{m}_j$ για οιουσδήποτε $i, j \in \{1, ..., n\}$, $i \neq j$, να αποδειχθούν τα εξής:

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

(ii) $\mathfrak{m}_1 \cap \mathfrak{m}_2 = \mathfrak{m}_1\mathfrak{m}_2$.

(iii) $(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n-1}) + \mathfrak{m}_n = R$.

(iv) $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cdots \mathfrak{m}_n$.

Εν συνεχεία, υποτιθεμένου ότι ο R είναι μια απειροπληθής ακεραία περιοχή έχουσα πεπερασμένου πλήθους αντιστρέψιμα στοιχεία, να αποδειχθούν και τα ακόλουθα:

(v) $\text{Rad}(\{0_R\}) = \{0_R\}$.

(vi) Ο R διαθέτει άπειρα σαφώς διακεκριμένα μεγιστικά ιδεώδη.

(vii) Στην ειδική περίπτωση όπου $R = \mathbb{Z}$, από το (vi) εξάγεται μια (επιπρόσθετη) απόδειξη για το ότι το σύνολο των πρώτων αριθμών είναι άπειρο.

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 $\text{Spec}(R)$. Για κάθε ιδεώδες I τού R εισάγουμε τον συμβολισμό:

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

Να αποδειχθούν τα ακόλουθα:

(i) $\text{Spec}(R) = \varnothing \iff$ 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) $\mathbf{V}(I) = \varnothing \iff I = R$.

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

(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

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

[*Σημείωση*: Είναι πρόδηλο εκ των ανωτέρω ότι το $\text{Spec}(R)$ εφοδιάζεται με μία *τοπολογία* έχουσα τα μέλη τής οικογενείας $\{\mathbf{V}(I) \mid I \text{ ιδεώδες τού } R\}$ ως *κλειστά σύνολα*. Η εν λόγω τοπολογία καλείται **τοπολογία Zariski** επί τού $\text{Spec}(R)$ 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

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

[*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) $\mathbf{V}(I) \subseteq \mathbf{V}(J) \iff \mathrm{Rad}(J) \supseteq \mathrm{Rad}(I)$.

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

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

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 $\nu \in \mathbb{N}$.

ΚΕΦΑΛΑΙΟ 3

Ομομορφισμοί δακτυλίων

Οι απεικονίσεις μεταξύ δυο δακτυλίων, οι οποίες τυγχάνει να μεταφέρουν τις εκάστοτε θεωρούμενες πράξεις προσθέσεως και πολλαπλασιασμού κατά τρόπο συμβατό, καλούνται *ομομορφισμοί δακτυλίων*. Οι *εμφυτεύσεις* δακτυλίων εντός άλλων διασφαλίζονται μέσω κατασκευής *μονομορφισμών*, ήτοι ενριπτικών ομομορφισμών. Οι *πυρήνες* των ομομορφισμών δακτυλίων αποτελούν ιδεώδη και κάθε ιδεώδες ενός δακτυλίου μπορεί να ιδωθεί ως πυρήνας τού λεγομένου *φυσικού επιμορφισμού*. Το *θεώρημα αντιστοιχίσεως* περιγράφει τον τρόπο συσχετισμού των ιδεωδών ενός δακτυλίου με τα ιδεώδη τής εικόνας αυτού μέσω ενός επιμορφισμού. Τέλος, τα *θεωρήματα ισομορφισμών* μάς παρέχουν χρήσιμες πληροφορίες για τις περιπτώσεις «ταυτίσεως» ορισμένων χαρακτηριστικών δακτυλίων και πηλικοδακτυλίων, κατ' αναλογίαν προς ό,τι συμβαίνει με τα συνώνυμα θεωρήματα περί ομάδων.

3.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

3.1.1 Ορισμός. Εάν οι $(R_1, +_1, \cdot_1)$ και $(R_2, +_2, \cdot_2)$ είναι δυο δακτύλιοι και

$$f : R_1 \longrightarrow R_2$$

μια απεικόνιση, τότε η f καλείται **ομομορφισμός (δακτυλίων)** όταν

$$\boxed{f(a +_1 b) = f(a) +_2 f(b)} \quad \text{και} \quad \boxed{f(a \cdot_1 b) = f(a) \cdot_2 f(b)} \tag{3.1}$$

για όλα τα $a, b \in R$.

Ένας ομομορφισμός δακτυλίων $f : R_1 \longrightarrow R_2$ ονομάζεται

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιρριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιρριπτική,
ενδομορφισμός (τού R_1)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$R_1 = R_2$,
αυτομορφισμός (τού R_1)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιρριπτικός ενδομορφισμός.

(Φυσικά, αυτές οι έννοιες εμπεριέχουν τις αντίστοιχες έννοιες για τις επί μέρους δομές, δηλαδή εκείνες των εκάστοτε μετεχουσών αβελιανών προσθετικών ομάδων και πολλαπλασιαστικών ημιομάδων).

3.1.2 Σημείωση. (Απλούστευση συμβολισμού.) Κατά κανόνα (για λόγους συντομίας) οι δείκτες $1, 2$ (ή οποιαδήποτε άλλη ειδική σήμανση) θα *παραλείπονται* στον συμβολισμό των πράξεων. Ωστόσο, θα πρέπει κανείς να έχει πάντα κατά νου το ποιο "$+$" και ποιο "$\cdot$" υπονοείται κατά περίπτωση.

3.1.3 Παραδείγματα. (i) Έστω m ένας φυσικός αριθμός. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \quad n \longmapsto [n]_m \, .$$

Είναι εύκολο να αποδειχθεί ότι η f είναι ένας επιμορφισμός δακτυλίων.

(ii) Η απεικόνιση $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f\,(n) := 2n$ *δεν είναι* ομομορφισμός δακτυλίων, παρότι *είναι* ισομορφισμός μεταξύ των αντιστοίχων προσθετικών ομάδων!

(iii) Έστω $(2\,\mathbb{Z}, +, \star)$ ο δακτύλιος ο αποτελούμενος από τους αρτίους ακεραίους με τη συνήθη πρόσθεση και τον ακόλουθο «τροποποιημένο» πολλαπλασιασμό:

$$m \star n := \frac{m \cdot n}{2} \, .$$

Τότε η $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f\,(n) := 2n$ (όπως και στο (ii)) αποτελεί *ισομορφισμό δακτυλίων.*

(iv) Εάν το K είναι ένα σώμα με $\text{χαρ}(K) = p > 0$, τότε η απεικόνιση

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

είναι ένας ενδομορφισμός (πρβλ. πρόταση 1.4.8 (i)) και καλείται, ιδιαιτέρως, **απεικόνιση τού Frobenius**.

(v) Ο ομομορφισμός

$$\mathbb{C} \longrightarrow \mathbb{C}, \;\; z = a + ib \longmapsto a - ib = \overline{z},$$

είναι ένας αυτομορφισμός τού σώματος των μιγαδικών αριθμών.

(vi) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \subsetneqq \mathbb{C}$$

το αριθμητικό τετραγωνικό σώμα το αντιστοιχιζόμενο στον m (βλ. άσκηση **1-44**). Τότε η απεικόνιση

$$f : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}(\sqrt{m}), \quad f(a + b\sqrt{m}) := a - b\sqrt{m},$$

αποτελεί έναν αυτομορφισμό τού $\mathbb{Q}(\sqrt{m})$ (βλ. άσκηση **3-5**).

(vii) Η *μηδενική απεικόνιση* $f : R \longrightarrow S$ μεταξύ δυο δακτυλίων R και S, όπου $f(a) = 0_S$ για κάθε $a \in R$, είναι ένας ομομορφισμός δακτυλίων (ο λεγόμενος **μηδενικός ομομορφισμός**). Σημειωτέον ότι όταν κανείς εκ των R, S δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιριπτικός.

(viii) Εάν $f : R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων και

$$\mathrm{in}_{\mathrm{Im}(f),S} : \mathrm{Im}(f) \longrightarrow S, \ s \longmapsto \mathrm{in}_{\mathrm{Im}(f),S}(s) := s,$$

η συνήθης ένθεση τής εικόνας του εντός τού S, τότε $f = \mathrm{in}_{\mathrm{Im}(f),S} \circ \check{f}$, όπου

$$\boxed{\check{f} : R \longrightarrow \mathrm{Im}(f), \ r \longmapsto \check{f}(r) := f(r),}$$

ο επιμορφισμός ο επαγόμενος μέσω τού f.

3.1.4 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Εάν $n \in \mathbb{N}$ και εάν τα $a_1, ..., a_n$ είναι στοιχεία τού R, τότε*

$$f(\sum_{j=1}^{n} a_j) = \sum_{j=1}^{n} f(a_j) \qquad \textit{και} \qquad f(\prod_{j=1}^{n} a_j) = \prod_{j=1}^{n} f(a_j).$$

ΑΠΟΔΕΙΞΗ. Έπεται κατόπιν χρήσεως των ισοτήτων (3.1) και μαθηματικής επαγωγής ως προς τον n. □

3.1.5 Πρόταση. *Ένας ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ έχει τις εξής ιδιότητες*:

(i) $f(0_R) = 0_{R'}$ *και* $f(-a) = -f(a), \ \forall a \in R$.

(ii) *Για κάθε $a \in R$ ισχύουν οι ισότητες*:

$$f(na) = n\, f(a), \ \forall n \in \mathbb{Z}, \ \textit{και} \ \ f(a^n) = f(a)^n, \ \forall n \in \mathbb{N}.$$

(iii) *Εάν ο S είναι ένας υποδακτύλιος τού R, τότε η εικόνα του $f(S)$ μέσω τής f είναι ένας υποδακτύλιος τού R'.*

(iv) *Εάν ο S' είναι ένας υποδακτύλιος τού R', τότε η αντίστροφή του εικόνα $f^{-1}(S')$ μέσω τής f είναι ένας υποδακτύλιος τού R.*

(v) *Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε και ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο, και μάλιστα ισχύει η ισότητα $f(1_R) = 1_{f(R)}$.*

(vi) *Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, η f μη μηδενικός ομομορφισμός και ο R' διαιρετικός δακτύλιος ή ακεραία περιοχή, τότε $f(1_R) = 1_{R'}$.*

(vii) *Εάν ο R είναι ένας μεταθετικός δακτύλιος, τότε και ο $f(R)$ είναι μεταθετικός.*

(viii) *Εάν ο R είναι ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και η f μη μηδενικός ομομορφισμός, τότε*

$$f(a^{-1}) \in f(R)^{\times},\ f(a^{-1}) = [f(a)]^{-1},\ \forall a \in R^{\times},$$

και, γενικότερα,

$$f(a^n) = f(a)^n,\ \forall a \in R^{\times} \text{ και } \forall n \in \mathbb{Z}.$$

(ix) *Εάν η f είναι μονομορφισμός και ο R ακεραία περιοχή (και αντιστοίχως, στεβλό σώμα/σώμα), τότε και ο $f(R)$ είναι ακεραία περιοχή (και αντιστοίχως, στρεβλό σώμα/σώμα).*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, οπότε ισχύει η ισότητα $f(0_R) = 0_{R'}$. Εξάλλου, για κάθε $a \in R$, έχουμε

$$0_{R'} = f(0_R) = f(a + (-a)) = f(a) + f(-a) \Longrightarrow f(-a) = -f(a).$$

(ii) Η απόδειξη έπεται από την πρόταση 3.1.4 και τη δεύτερη ισότητα τού (i).

(iii) Εάν $b_1, b_2 \in f(S)$, τότε υπάρχουν $a_1, a_2 \in S$, τέτοια ώστε $f(a_1) = b_1$ και $f(a_2) = b_2$. Επειδή ο S είναι ένας υποδακτύλιος τού R,

$$\left.\begin{array}{r} a_1 - a_2 \in S, \\ a_1 a_2 \in S \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in f(S), \\ b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(S), \end{array}\right.$$

οπότε η εικόνα $f(S)$ τού S μέσω τής f είναι όντως ένας υποδακτύλιος τού R'.

(iv) Εάν $a_1, a_2 \in f^{-1}(S')$, τότε $f(a_1) \in S'$ και $f(a_2) \in S'$. Κι επειδή ο S' είναι υποδακτύλιος τού R',

$$\left.\begin{array}{r} f(a_1 - a_2) = f(a_1) - f(a_2) \in S', \\ f(a_1 a_2) = f(a_1) f(a_2) \in S' \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a_1 - a_2 \in f^{-1}(S'), \\ a_1 a_2 \in f^{-1}(S'), \end{array}\right.$$

ήτοι *και* η αντίστροφή του εικόνα $f^{-1}(S')$ μέσω τής f είναι ένας υποδακτύλιος τού δακτυλίου R.

(v) Έστω b τυχόν στοιχείο τού $f(R)$. Τότε υπάρχει ένα $a \in R$, τέτοιο ώστε να ισχύει η ισότητα $f(a) = b$. Άρα

$$f(1_R) f(a) = f(1_R a) = f(a), \quad f(a) f(1_R) = f(a 1_R) = f(a),$$

οπότε ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο και $f\left(1_R\right) = 1_{f(R)}$.

(vi) Επειδή -εξ υποθέσεως- ο f δεν είναι ο μηδενικός ομομορφισμός, θα υπάρχει ένα $a \in R$, τέτοιο ώστε $f(a) \neq 0_{R'}$. Εξ αυτού έπεται ότι

$$f(a) \cdot 1_{R'} = f(a) = f(a \cdot 1_R) = f(a)f(1_R) \Longrightarrow f(a)\left(f\left(1_R\right) - 1_{R'}\right) = 0_{R'}.$$

Εάν ο R' είναι διαιρετικός δακτύλιος, τότε υπάρχει το αντίστροφο $f(a)^{-1}$ τού $f(a)$, με το οποίο μπορούμε να πολλαπλασιάσουμε αμφότερα τα μέλη τής ανωτέρω ισότητας και να λάβουμε $f\left(1_R\right) = 1_{R'}$. Εάν, από την άλλη μεριά, ο R' είναι ακεραία περιοχή, τότε μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα κάνοντας χρήση τού νόμου τής διαγραφής 1.2.5.

(vii) Προφανώς, για κάθε $a, b \in R$, έχουμε

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

(viii) Για κάθε $a \in R^\times$ έχουμε

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_R) = f(a^{-1}a) = f(a^{-1})f(a).$$

Κι επειδή (λόγω το (v)) ισχύει $f\left(1_R\right) = 1_{f(R)} \neq 0_{R'}$, έχουμε $f(a) \neq 0_{R'}$ και $f(a^{-1}) = \left[f\left(a\right)\right]^{-1} \in f\left(R\right)^\times$. Η δεύτερη ισότητα αποδεικνύεται εύκολα μέσω μαθηματικής επαγωγής.

(ix) Έστω ότι ο f είναι μονομορφισμός και ο R ακεραία περιοχή. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Εάν υποθέσουμε ότι $f(a), f(b) \in f(R)$, για κάποια $a, b \in R$, τέτοια ώστε να ισχύει

$$f(a)f(b) = 0_{f(R)} \Longleftrightarrow f(ab) = 0_{f(R)} = f\left(0_R\right),$$

τότε $ab = 0_R$, οπότε $a = 0_R$ ή $b = 0_R$. Συνεπώς, $f(a) = 0_{f(R)}$ ή $f(b) = 0_{f(R)}$. Άρα *και* ο $f(R)$ είναι ακεραία περιοχή.

Εν συνεχεία, ας υποθέσουμε ότι ο f είναι μονομορφισμός και ο R στρεβλό σώμα. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Αρκεί λοιπόν να δείξουμε ότι $f(R)^\times = f(R) \setminus \{0_{R'}\}$. Ο εγκλεισμός "$\subseteq$" είναι πρόδηλος. Ας θεωρήσουμε τυχόν $b \in f(R) \setminus \{0_{R'}\}$. Τότε υπάρχει ένα $a \in R \setminus \{0_R\}$, τέτοιο ώστε $b = f(a)$. Όμως -εξ υποθέσεως- $R \setminus \{0_R\} = R^\times$, οπότε $a \in R^\times$, πράγμα που σημαίνει ότι υπάρχει (πολλαπλασιαστικό) αντίστροφο a^{-1} τού a, για το οποίο ισχύει $f(a^{-1}) = \left[f\left(a\right)\right]^{-1} \in f\left(R\right)^\times$ (βάσει τού (viii)). Άρα $b \in f(R)^\times$, και, ως εκ τούτου, ο $f(R)$ είναι στρεβλό σώμα. (Στην περίπτωση κατά την οποία ο f είναι μονομορφισμός και ο R σώμα, αρκεί να χρησιμοποιήσουμε ό,τι προείπαμε σε συνδυασμό με το (vii).) □

3.1.6 Πρόταση. *Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ομομορφισμοί* (*και αντιστοίχως, μονομορφισμοί/επιμορφισμοί/ισομορφισμοί*) *δακτυλίων, και η σύνθεσή τους $g \circ f : R \longrightarrow R''$ θα είναι ομομορφισμός* (*και αντιστοίχως, μονομορφισμός/επιμορφισμός/ισομορφισμός*) *δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Εάν οι f και g είναι ομομορφισμοί δακτυλίων, τότε για όλα τα $a, b \in R$ ισχύουν οι ισότητες

$$(g \circ f)(a+b) = g(f(a+b)) = g(f(a) + f(b))$$
$$= g(f(a)) + g(f(b)) = (g \circ f)(a) + (g \circ f)(b)$$

και

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)\, f(b))$$
$$= g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b),$$

οπότε και η σύνθεσή τους $g \circ f$ είναι ένας ομομορφισμός δακτυλίων. Η απόδειξη αποπερατούται λαμβάνοντας υπ' όψιν το γεγονός ότι η σύνθεση δυο ενρίψεων (και αντιστοίχως, επιρρίψεων/αμφιρρίψεων) είναι μια ένριψη (και αντιστοίχως, μια επίρριψη/αμφίρριψη). □

3.1.7 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι, τότε γράφουμε[1] $R \cong R'$ και λέμε ότι **ο R είναι ισόμορφος με τον R'** (ή ότι οι R και R' **είναι ισόμορφοι**) όταν υπάρχει κάποιος ισομορφισμός δακτυλίων $f : R \longrightarrow R'$. (Κατ' αναλογίαν, το σύμβολο $R \ncong R'$ δηλοί ότι ο δακτύλιος R *δεν είναι ισόμορφος* με τον R'.)

3.1.8 Παραδείγματα. (i) Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ (βλ. άσκηση **1-44**) είναι ισόμορφη με τον ακόλουθο δακτύλιο 2×2-πινάκων:

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

καθόσον υφίσταται ισομορφισμός δακτυλίων:

$$\mathbb{Z}[\sqrt{2}] \ni a + b\sqrt{2} \longmapsto \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in R.$$

(ii) Έχουμε $\mathbb{Z}[\sqrt{2}] \ncong \mathbb{Z}[\sqrt{3}]$, διότι εάν υπήρχε ισομορφισμός δακτυλίων

$$f : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}],$$

θα έπρεπε να ισχύει

$$f(\sqrt{2})^2 = f((\sqrt{2})^2) = f(2) = f(1+1) = 2f(1) = 2 \Rightarrow f(\sqrt{2}) \in \{\pm\sqrt{2}\},$$

κάτι που θα αντέφασκε προς το ότι $\pm\sqrt{2} \notin \mathbb{Z}[\sqrt{3}]$.

(iii) Τα σώματα $\mathbb{C}$ και $\mathbb{R}$ δεν είναι ισόμορφα, διότι εάν υπήρχε ένας ισομορφισμός $f : \mathbb{C} \longrightarrow \mathbb{R}$, τότε θα έπρεπε να ισχύει

$$-1 = -f(1) = f(-1) = f(i^2) = f(i)^2$$

(όπου i η φανταστική μονάδα), κάτι που θα αντέφασκε προς το ότι $f(i) \in \mathbb{R}$.

[1] Από τούδε και στο εξής μέσω τού συμβόλου "$\cong$" θα εκφράζουμε την ύπαρξη ισομορφισμών *δακτυλίων*. Ωστόσο, επειδή (στη Θεωρία Ομάδων) χρησιμοποιήσαμε το *ίδιο* σύμβολο *και* για τους ισομορφισμούς *ομάδων*, οφείλουμε να είμαστε ιδιάτερα προσεκτικοί (πρβλ. 3.1.3 παράδειγμα (ii)). Σε περίπτωσεις στις οποίες ενδέχεται να προκληθεί σύγχυση, θα μπορούσε κανείς να χρησιμοποιήσει τα (κάπως δυσμετακίνητα) σύμβολα $\underset{\text{δακτ.}}{\cong}$ και $\underset{\text{ομάδ.}}{\cong}$, αντιστοίχως.

3.1.9 Πρόταση. *Για οιουσδήποτε δακτυλίους* R, R', R'' *ισχύουν τα εξής*:

(i) $R \cong R$,

(ii) $R \cong R' \Longrightarrow R' \cong R$,

(iii) $[R \cong R' \text{ και } R' \cong R''] \Longrightarrow R \cong R''$.

ΑΠΟΔΕΙΞΗ. (i) Η ταυτοτική απεικόνιση $\mathrm{id}_R : R \to R$ είναι προφανώς ένας ισομορφισμός δακτυλίων.

(ii) Εάν ο $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε, ως αμφιρριπτική απεικόνιση, θα διαθέτει μια (μονοσημάντως ορισμένη, αμφιρριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} αποτελεί ομομορφισμό δακτυλίων. Εάν $x, y \in R'$, τότε υπάρχουν $a, b \in R$ με $x = f(a)$ και $y = f(b)$. Επομένως,

$$\begin{cases} f^{-1}(x+y) = f^{-1}(f(a)+f(b)) = f^{-1}(f(a+b)) = a+b = f^{-1}(x) + f^{-1}(y), \\ f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)\, f^{-1}(y), \end{cases}$$

(αφού οι f, f^{-1} αμφιρριπτικές) και η f^{-1} είναι όντως ομομορφισμός δακτυλίων.

(iii) Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ισομορφισμοί δακτυλίων, τότε, σύμφωνα με την πρόταση 3.1.6, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός δακτυλίων. □

3.1.10 Σημείωση. Σύμφωνα με την πρόταση 3.1.9, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από δακτυλίους (ή επί τής NBG-«κλάσεως» *όλων* των δακτυλίων). Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο δακτύλιοι λογίζονται ως (δακτυλιοθεωρητικώς) *ταυτιζόμενοι* όταν είναι μεταξύ τους ισόμορφοι, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο δακτυλιοθεωρητικός προσδιορισμός μιας οικογενείας δακτυλίων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού* [2].

3.1.11 Πόρισμα. *Εάν οι* R *και* R' *είναι δυο δακτύλιοι και* $R \cong R'$, *τότε ισχύουν τα εξής*:

(i) *Ο* R *είναι ακεραία περιοχή* $\Leftrightarrow$ *ο* R' *είναι ακεραία περιοχή.*

(ii) *Ο* R *είναι στεβλό σώμα* $\Leftrightarrow$ *ο* R' *είναι στεβλό σώμα.*

(iii) *Ο* R *είναι σώμα* $\Leftrightarrow$ *ο* R' *είναι σώμα.*

ΑΠΟΔΕΙΞΗ. Εάν η $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε αρκεί να εφαρμοσθεί το (ix) τής προτάσεως 3.1.5 για αμφότερες τις f και f^{-1}. (Πρβλ. με το (ii) τής προτάσεως 3.1.9.) □

[2] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (δακτυλίων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

3.1.12 Πρόταση. *Εάν ο $f : K \longrightarrow R$ είναι ένας ομομορφισμός δακτυλίων, όπου ο K είναι ένας διαιρετικός δακτύλιος* (= *στρεβλό σώμα*), *τότε ο f είναι ή ο μηδενικός ομομορφισμός ή ένας μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Εάν ο R είναι τετριμμένος δακτύλιος, τότε ο f είναι κατ' ανάγκην ο μηδενικός ομομορφισμός. Εάν ο R είναι μη τετριμμένος δακτύλιος και ο f δεν είναι ο μηδενικός ομομορφισμός (ήτοι δεν ισχύει $f(a) = 0_R$, *για κάθε* $a \in K$), και εάν -επιπροσθέτως- υποθέσουμε ότι $f(x) = f(y)$ για κάποια $x, y \in K$, τότε

$$f(x - y) = f(x) - f(y) = 0_R. \tag{3.2}$$

Εάν $x-y \neq 0_K$, τότε το $x-y$ θα διαθέτει πολλαπλασιαστικό αντίστροφο $(x-y)^{-1}$. Αυτό, κατά το (viii) τής προτάσεως 3.1.5, σημαίνει ότι

$$f((x-y)^{-1}) \in f\,(K)^{\times}\,, \;\; f((x-y)^{-1}) = (f(x-y))^{-1}. \tag{3.3}$$

Από τις (3.2) και (3.3) συνάγεται ότι $0_R = f(x-y)(f(x-y))^{-1} = 1_R$, πράγμα άτοπο. Επομένως, $x = y$, και ο f είναι κατ' ανάγκην μονομορφισμός. □

3.1.13 Πόρισμα. *Κάθε επιμορφισμός στρεβλών σωμάτων $f : K \longrightarrow L$ είναι ισομορφισμός.*

ΑΠΟΔΕΙΞΗ. Επειδή ο πληθικός αριθμός τού L είναι ≥ 2 και ο f επιμορφισμός, ο f αδυνατεί να είναι ο τετριμμένος ομομορφισμός. Κατά συνέπειαν, ο f οφείλει να είναι *και* ενριπτικός επί τη βάσει τής προτάσεως 3.1.12. □

3.1.14 Ορισμός. Εάν ο $f : R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων, τότε ο υποδακτύλιος $\mathrm{Ker}(f) := f^{-1}(\{0_{R'}\})$ τού R ονομάζεται **πυρήνας** τού f.

3.1.15 Πρόταση. *Ο πυρήνας* $\mathrm{Ker}(f)$ *ενός ομομορφισμού δακτυλίων $f : R \to R'$ αποτελεί ένα ιδεώδες τού R.*

ΑΠΟΔΕΙΞΗ. Έστω ότι $r \in R$ και ότι $a, b \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{aligned} f(a-b) = f(a) - f(b) = 0_{R'} - 0_{R'} = 0_{R'}, \\ f(ar) = f(a)f(r) = 0_{R'} f(r) = 0_{R'}, \\ f(ra) = f(r)f(a) = f(r)0_{R'} = 0_{R'} \end{aligned}\right\} \Longrightarrow a-b,\ ar,\ ra \in \mathrm{Ker}(f).$$

Άρα ο $\mathrm{Ker}(f)$ είναι εξ ορισμού ένα ιδεώδες τού R. □

3.1.16 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Τότε ο*

$$f \text{ είναι μονομορφισμός} \iff \mathrm{Ker}\,(f) = \{0_R\}\ .$$

ΑΠΟΔΕΙΞΗ. Εάν ο f είναι μονομορφισμός δακτυλίων και a είναι ένα τυχόν στοιχείο τού πυρήνα $\mathrm{Ker}(f)$, τότε

$$f(a) = 0_{R'} = f(0_R) \underset{f \text{ ένριψη}}{\Longrightarrow} a = 0_R.$$

Άρα $\mathrm{Ker}(f) = \{0_R\}$. Και αντιστρόφως· εάν ισχύει $\mathrm{Ker}(f) = \{0_R\}$ και υποθέσουμε ότι $f(x) = f(y)$, για κάποια $x, y \in R$, τότε

$$f(x-y) = f(x) - f(y) = 0_{R'} \Longrightarrow x - y \in \mathrm{Ker}(f) = \{0_R\} \Longrightarrow x - y = 0_R,$$

δηλαδή ο ομομορφισμός f είναι ενριπτικός. □

3.1.17 Ορισμός. Λέμε ότι ο δακτύλιος R μπορεί να **εμφυτευθεί** (ή ότι είναι **εμφυτεύσιμος**) σε έναν δακτύλιο R' όταν υπάρχει ένας μονομορφισμός δακτυλίων $f : R \longrightarrow R'$.

3.1.18 Πρόταση. *Ένας δακτύλιος R είναι εμφυτεύσιμος σε έναν δακτύλιο R' εάν και μόνον εάν ο R είναι ισόμορφος με έναν υποδακτύλιο τού R'.*

ΑΠΟΔΕΙΞΗ. Εάν ένας δακτύλιος R είναι εμφυτεύσιμος σε έναν δακτύλιο R', τότε υφίσταται κάποιος μονομορφισμός $f : R \longrightarrow R'$. Επομένως, ο μέσω αυτού επαγόμενος επιμορφισμός $\check{f} : R \longrightarrow \mathrm{Im}(f)$ (βλ. 3.1.3 (viii)) είναι ισομορφισμός. Και αντιστρόφως· εάν ο R είναι ισόμορφος με έναν υποδακτύλιο S τού R', τότε υφίσταται κάποιος ισομορφισμός $f : R \longrightarrow S$. Θεωρώντας (κατόπιν επεκτάσεως) ως πεδίο τιμών τής απεικονίσεως f το R' λαμβάνουμε τον μονομορφισμό δακτυλίων $R \ni r \longmapsto f(r) \in R'$. □

3.1.19 Πρόταση. *Κάθε δακτύλιος R μπορεί να εμφυτευθεί (όχι μονοσημάντως) σε έναν δακτύλιο R' με μοναδιαίο στοιχείο. Μάλιστα, ο R' μπορεί να επιλεγεί κατά τέτοιον τρόπο, ώστε* $\mathrm{χαρ}(R') = 0$ *ή* $\mathrm{χαρ}(R') = \mathrm{χαρ}(R)$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε το καρτεσιανό γινόμενο $R' := \mathbb{Z} \times R$, όπου $\mathbb{Z}$ ο δακτύλιος των ακεραίων αριθμών. Επί τού R' ορίζονται πράξεις προσθέσεως και πολλαπλασιασμού ως ακολούθως:

(i) $(m, a) + (n, b) := (m + n, a + b)$,

(ii) $(m, a) \cdot (n, b) := (mn, mb + na + ab)$,

για οιαδήποτε $(m, a), (n, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής 0 με μοναδιαίο του στοιχείο το $(1, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto (0, a)\,,$$

είναι ένας μονομορφισμός. Εάν $\mathrm{χαρ}(R) = k > 0$, τότε μπορούμε να θεωρήσουμε ως R' το καρτεσιανό γινόμενο $R' := \mathbb{Z}_k \times R$ εφοδιασμένο με τις πράξεις:

(i) $([m]_k\,, a) + ([n]_k\,, b) := ([m + n]_k\,, a + b)$,

(ii) $([m]_k, a) \cdot ([n]_k, b) := ([mn]_k, mb + na + ab)$,
για κάθε $([m]_k, a), ([n]_k, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής k με μοναδιαίο του στοιχείο το $([1]_k, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto ([0]_k, a),$$

είναι και πάλι ένας μονομορφισμός. □

3.1.20 Σημείωση. Πολλές φορές συμβαίνει «ειδικοί» δακτύλιοι να είναι εμφυτευμένοι σε δακτυλίους «ολιγότερο ειδικούς». Επί παραδείγματι, σώματα ενδέχεται να είναι εμφυτευμένα εντός στρεβλών σωμάτων, και ακέραιες περιοχές εντός δακτυλίων με μηδενοδιαιρέτες (βλ. 3.1.21 (i) και (ii)). Ωστόσο, όπως θα δούμε στην ενότητα 3.5 (βλ. πρόταση 3.5.7), *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί κατά τρόπο φυσικό σε ένα σώμα.

3.1.21 Παραδείγματα. (i) Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι εμφυτευμένο στο στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$ των (πραγματικών) τετρανίων (οπότε το $\mathbb{H}_{\mathbb{R}}$ μπορεί, υπό μία άποψη, να θεωρείται ως «φυσική επέκταση» τού $\mathbb{C}$) μέσω τού ακόλουθου μονομορφισμού:

$$\boxed{\mathbb{C} \hookrightarrow \mathbb{H}_{\mathbb{R}}, \;\; a + bi \longmapsto a\mathbf{I} + b\mathbf{J} = \begin{pmatrix} a + bi & 0 \\ 0 & a - bi \end{pmatrix},}$$

όπου οι **I** και **J** είναι οι πίνακες οι εισαχθέντες στο 1.2.19 (ii).

(ii) Εάν στην πρόταση 3.1.19 θέσουμε $R := \mathbb{Z}$ και $R' := \mathbb{Z} \times \mathbb{Z}$ (με τη δομή δακτυλίου την ορισθείσα κατά την αποδεικτική διαδικασία!), τότε ο R είναι ακεραία περιοχή, ενώ ο R' *δεν είναι*, διότι π.χ. για κάθε $n \in \mathbb{Z} \smallsetminus \{0\}$ ισχύει η ισότητα:

$$(-2, 2)\,(0, 2n) = (0, 0 - 4n + 4n) = (0, 0).$$

► **Πηλικοδακτύλιοι και φυσικοί επιμορφισμοί**. Έστω R ένας δακτύλιος και έστω I ένα ιδεώδες αυτού. Θεωρούμε τον *πηλικοδακτύλιο* R/I (βλ. 2.6.1 και 2.6.2). Η απεικόνιση

$$\boxed{\pi_I^R : R \longrightarrow R/I, \;\; \pi_I^R(r) := r + I, \; \forall r \in R,} \tag{3.4}$$

είναι προφανώς επιρριπτική.

3.1.22 Λήμμα. *Η* (3.4) *αποτελεί έναν επιμορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τις (2.7) και (2.8). □

3.1.23 Ορισμός. Η (3.4) καλείται **φυσικός επιμορφισμός** (ή **επιμορφισμός κλάσεων υπολοίπων**) τού R επί τού πηλικοδακτυλίου R/I.

Η επόμενη πρόταση δηλοί -κατ' ουσίαν- ότι οι έννοιες «πυρήνας ομομορφισμού δακτυλίων» και «ιδεώδες» μπορούν να χρησιμοποιούνται η μία αντί τής άλλης χωρίς περαιτέρω περιορισμούς.

3.1.24 Πρόταση. *Έστω R τυχών δακτύλιος. Τότε ένα υποσύνολο $\varnothing \neq I \subseteq R$ αποτελεί ένα ιδεώδες τού R εάν και μόνον εάν το I είναι ο πυρήνας ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ (για κάποιον κατάλληλο δακτύλιο S).*

ΑΠΟΔΕΙΞΗ. Εάν $\varnothing \neq I \subseteq R$ είναι ένα ένα ιδεώδες τού R, τότε ο φυσικός επιμορφισμός (3.4) έχει ως πυρήνα του τον $\mathrm{Ker}(\pi_I^R) = \{r \in R \mid r + I = I\} = I$. Το αντίστροφο είναι άμεση συνέπεια τής προτάσεως 3.1.15. □

3.1.25 Πόρισμα. *Ο φυσικός επιμορφισμός* (3.4) *είναι ισομορφισμός εάν και μόνον εάν $I = \{0_R\}$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση 3.1.16 ο $\pi_I^R : R \longrightarrow R/I$ είναι μονομορφισμός εάν και μόνον εάν ο πυρήνας του (που ισούται με το I) είναι το τετριμμένο ιδεώδες. □

3.1.26 Πόρισμα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο R είναι ένα σώμα.*

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

(iii) *Το $\{0_R\}$ είναι μεγιστικό ιδεώδες τού R.*

(iv) *Κάθε μη μηδενικός ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ είναι μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Η αμφίπλευρη συνεπαγωγή (i)⇔(ii) έπεται από το πόρισμα 2.1.11, η (i)⇔(iii) από το πόρισμα 2.6.5 (αφού $R \cong R/\{0_R\}$, βλ. 3.1.11 (iii) και 3.1.25) και η συνεπαγωγή (i)⇒(iv) από την πρόταση 3.1.12. Για την απόδειξη τής συνεπαγωγής (iv)⇒(ii) αρκεί να θεωρήσουμε *τυχόν* ιδεώδες $I \subsetneqq R$ και τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$, ο οποίος είναι μη μηδενικός με $\mathrm{Ker}(\pi_I^R) = I$. Εάν υποθέσουμε ότι ο π_I^R είναι μονομορφισμός, έχουμε $I = \{0_R\}$, οπότε ο R δεν διαθέτει άλλα γνήσια ιδεώδη πέραν τού τετριμμένου. Η απόδειξη λήγει ακολουθώντας τις συνεπαγωγές (iv)⇒(ii)⇒(i). □

3.2 ΘΕΩΡΗΜΑ ΑΝΤΙΣΤΟΙΧΙΣΕΩΣ ΙΔΕΩΔΩΝ

3.2.1 Λήμμα. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Εάν υποτεθεί ότι το I είναι ένα* (αριστερό/δεξιό/αμφίπλευρο) *ιδεώδες τού R και το J ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού S, τότε ισχύουν τα ακόλουθα*:

(i) *Η εικόνα $f(I)$ τού I μέσω τού f είναι ένα* (αριστερό/δεξιό/αμφίπλευρο) *ιδεώδες*

τού δακτυλίου $f(R)$.

(ii) *Η αντίστροφη εικόνα* $f^{-1}(J)$ *τού* J *μέσω τού* f *είναι ένα* (*αριστερό/ δεξιό/αμφίπλευρο*) *ιδεώδες τού* R.

ΑΠΟΔΕΙΞΗ. (i) Θεωρούμε τυχόντα στοιχεία $s \in f(R)$ και $x, y \in f(I)$. Επειδή το I είναι (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R, υπάρχουν $r \in R$, $a, b \in I$, τέτοια ώστε $s = f(r)$, $x = f(a)$ και $y = f(b)$, και ισχύουν τα ακόλουθα:

$$\left.\begin{array}{r} x - y = f(a) - f(b) = f(a-b) \in f(I), \\ sx = f(r)f(a) = f(ra) \in f(I) \mid\ xs = f(ar) \in f(I) \ \mid\ sx, xs \in f(I) \end{array}\right\}$$

απ' όπου έπεται ότι η εικόνα $f(I)$ τού I μέσω τού f είναι ένα (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού δακτυλίου $f(R)$.

(ii) Θεωρούμε τυχόντα στοιχεία $r \in R$ και $a, b \in f^{-1}(J)$. Τότε, επειδή το J είναι (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού S,

$$\left.\begin{array}{r} f(a-b) = f(a) - f(b) \in J, \\ f(ra) = f(r)f(a) \in J \ \mid\ f(ar) = f(a)f(r) \in J \ \mid\ f(ra), f(ar) \in J \end{array}\right\}$$

απ' όπου έπεται ότι $a - b,\ ra \mid\ ar \mid\ ra, ar \in f^{-1}(J)$. Άρα το $f^{-1}(J)$ είναι εξ ορισμού ένα ομοειδές ιδεώδες τού R. □

3.2.2 Σημείωση. Εάν υποτεθεί ότι το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και ότι ο f δεν είναι επιμορφισμός, η εικόνα $f(I)$ τού I μέσω τού f είναι ένα ομοειδές ιδεώδες τού δακτυλίου $f(R)$ αλλά όχι κατ' ανάγκην και τού S. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, η εικόνα τού ιδεώδους $I := 2\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών μέσω αυτής είναι το υποσύνολο $2\mathbb{Z}$ τού $\mathbb{Q}$ που *δεν είναι ιδεώδες* τού σώματος των ρητών αριθμών (καθότι τα μόνα ιδεώδη τού $\mathbb{Q}$ είναι τα $\{0\}$ και $\mathbb{Q}$, βλ. πόρισμα 2.1.11).

3.2.3 Πρόταση. *Έστω* I *ένα* (*αριστερό/δεξιό/αμφίπλευρο*) *ιδεώδες ενός δακτυλίου* R *και έστω* J *ένα* (*αριστερό/δεξιό/αμφίπλευρο*) *ιδεώδες ενός δακτυλίου* S. *Για κάθε ομομορφισμό δακτυλίων* $f : R \longrightarrow S$ *ισχύουν τα εξής*:

(i) $f\left(I \cap f^{-1}(J)\right) = f(I) \cap J$.

(ii) $f\left(f^{-1}(J)\right) = \mathrm{Im}(f) \cap J$.

(iii) $f^{-1}(J + f(I)) = f^{-1}(J) + I$.

(iv) $f^{-1}(f(I)) = \mathrm{Ker}(f) + I$.

ΑΠΟΔΕΙΞΗ. (i) Για κάθε $r \in f^{-1}(J)$ έχουμε $f(r) \in J$, οπότε $f\left(f^{-1}(J)\right) \subseteq J$. Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής τής απεικονίσεως f, έχουμε

$$\left.\begin{array}{r} f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \\ f\left(I \cap f^{-1}(J)\right) \subseteq f\left(f^{-1}(J)\right) \end{array}\right\} \Longrightarrow f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \cap J.$$

Έστω τώρα τυχόν $s \in f(I) \cap J$. Προφανώς, $s \in J$ και $s = f(r)$ για κάποιο στοιχείο $r \in I$. Επειδή $f(r) \in J$, έχουμε $s \in f\left(I \cap f^{-1}(J)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f(I) \cap J \subseteq f\left(I \cap f^{-1}(J)\right).$$

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $I = R$.
(iii) Για κάθε $a \in I$ έχουμε $f(a) \in f(I)$. Επομένως, $I \subseteq f^{-1}(f(I))$. Από το (ii) και από το γεγονός ότι οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν θεωρήσεως αντιστρόφων εικόνων προκύπτει ότι

$$f^{-1}(J) + I \subseteq f^{-1}\left(f(f^{-1}(J) + I)\right) = f^{-1}\left(f(f^{-1}(J)) + f(I)\right) \subseteq f^{-1}(J + f(I)).$$

Έστω τώρα τυχόν $r \in f^{-1}(J + f(I))$. Επειδή $f(r) \in J + f(I)$, υπάρχουν $s \in J$ και $b \in I$, τέτοια ώστε $f(r) = s + f(b)$. Κατά συνέπειαν,

$$f(r + (-b)) = s \in J \Rightarrow r + (-b) \in f^{-1}(s) \subseteq f^{-1}(J) \Rightarrow r \in f^{-1}(J) + I,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f^{-1}(J + f(I)) \subseteq f^{-1}(J) + I.$$

(iv) Αρκεί να εφαρμοσθεί το (iii) στην ειδική περίπτωση όπου $J = \{0_S\}$. □

3.2.4 Θεώρημα τής αντιστοιχίσεως. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων και έστω $W := \mathrm{Ker}(f)$. Τότε η*

$$\left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } R \\ \text{που περιέχουν τον } W \end{array} \right\} \xrightarrow{\alpha} \left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } S \end{array} \right\}$$

η οριζόμενη από τον τύπο

$$\boxed{I \longmapsto \alpha(I) := f(I)}$$

είναι μια αμφίρριψη που διατηρεί τους εγκλεισμούς, δηλαδή για οιαδήποτε ιδεώδη I_1, I_2 τού R ισχύει η συνεπαγωγή

$$W \subseteq I_1 \subsetneqq I_2 \Longrightarrow \alpha(I_1) \subsetneqq \alpha(I_2).$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε την

$$\left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } S \end{array} \right\} \xrightarrow{\beta} \left\{ \begin{array}{c} \text{αριστερά/δεξιά/αμφίπλευρα} \\ \text{ιδεώδη τού } R \\ \text{που περιέχουν τον } W \end{array} \right\}$$

την οριζόμενη από τον τύπο

$$J \longmapsto \beta(J) := f^{-1}(J).$$

Το ότι οι α, β είναι καλώς ορισμένες απεικονίσεις έπεται από το λήμμα 3.2.1. Για κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες J τού S λαμβάνουμε

$$\alpha(\beta(J)) = \alpha(f^{-1}(J)) = f(f^{-1}(J)) = \mathrm{Im}(f) \cap J = S \cap J = J$$

(βλ. 3.2.3 (ii)). Κατά συνέπειαν,

$$\alpha(\beta(J)) = J. \tag{3.5}$$

Από την άλλη μεριά, για κάθε ιδεώδες (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες I τού R που περιέχει τον πυρήνα W τού f λαμβάνουμε

$$\beta(\alpha(I)) = \beta(f(I)) = f^{-1}(f(I)) = W + I = I$$

(βλ. 3.2.3 (iv)). Κατά συνέπειαν,

$$\beta(\alpha(I)) = I. \tag{3.6}$$

Από τις (3.5) και (3.6) συμπεραίνουμε ότι η απεικόνιση α είναι αμφιρριπτική έχουσα την β ως αντίστροφό της. Τέλος, ας υποθέσουμε ότι τα I_1, I_2 είναι δυο (αριστερά/δεξιά/αμφίπλευρα) ιδεώδη τού R τα οποία περιέχουν τον W και για τα οποία ισχύει ο εγκλεισμός $I_1 \subsetneqq I_2$. Προφανώς, $f(I_1) \subseteq f(I_2)$. Κι επειδή

$$f(I_1) = f\,(I_2) \Rightarrow I_1 = f^{-1}(f(I_1)) = f^{-1}(f(I_2)) = I_2,$$

έχουμε $\alpha(I_1) = f(I_1) \subsetneqq f(I_2) = \alpha(I_1)$. □

3.2.5 Πόρισμα. *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε κάθε ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής J/I, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$ (βλ. (3.4)). Βάσει τού θεωρήματος 3.2.4 τής αντιστοιχίσεως ιδεωδών κάθε ιδεώδες τού R/I είναι τής μορφής $\pi_I^R(J)$, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το $I = \mathrm{Ker}(\pi_I^R)$ (βλ. πρόταση 3.1.24). Το I είναι και αυτό ένα ιδεώδες τού J (όταν το J θεωρηθεί αφ' εαυτού ως δακτύλιος αναφοράς), ενώ η εικόνα $\pi_I^R(J)$ ισούται με

$$\pi_I^R(J) = \left\{ \pi_I^R(a) \;\middle|\; a \in J \right\} = \{ a + I \mid a \in J \} = J/I,$$

απ' όπου έπεται το ζητούμενο. □

3.2.6 Παράδειγμα. Για $R = \mathbb{Z}$ και $I = m\mathbb{Z}$, $m \in \mathbb{N}$, το σύνολο των ιδεωδών τού πηλικοδακτυλίου $\mathbb{Z}/m\mathbb{Z}$ είναι το

$$\{\, d\mathbb{Z}/m\mathbb{Z} \mid\ d \in \mathbb{N} \text{ και } d \mid m \,\}.$$

3.3 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Αυτά είναι τρία χαρακτηριστικά θεωρήματα (βλ. 3.3.3, 3.3.16 και 3.3.21) τα οποία περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών δακτυλίων, των ιδεωδών δακτυλίων και των πηλικοδακτυλίων. Τα εξ αυτών εξαγόμενα πορίσματα είναι πολιποίκιλα και λίαν χρήσιμα.

3.3.1 Λήμμα. *Εάν τα A, B είναι μη κενά σύνολα και η $\pi : A \longrightarrow B$ μια απεικόνιση, τότε τα ακόλουθα είναι ισοδύναμα*:

(i) *Η π είναι επιρριπτική απεικόνιση.*

(ii) *Υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$.*

(iii) *Η π είναι «εκ δεξιών διαγράψιμη», δηλαδή για οιοδήποτε μη κενό σύνολο C και οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ ισχύει η συνεπαγωγή*

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η π είναι επιρριπτική απεικόνιση, τότε για κάθε στοιχείο $y \in B = \mathrm{Im}(\pi) = \pi(A)$ επιλέγουμε ένα $x_y \in A$, ούτως ώστε να ισχύει $\pi(x_y) = y$, και ορίζουμε την απεικόνιση $\gamma : B \longrightarrow A,\ y \longmapsto \gamma(y) := x_y$. Τότε

$$(\pi \circ \gamma)(y) = \pi(\gamma(y)) = \pi(x_y) = y = \mathrm{id}_B(y) \Longrightarrow \pi \circ \gamma = \mathrm{id}_B.$$

(ii)⇒(iii) Υποθέτουμε ότι υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$. Για οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ για τις οποίες ισχύει η ισότητα $h_1 \circ \pi = h_2 \circ \pi$ λαμβάνουμε

$$\begin{aligned} h_1 \circ \pi &= h_2 \circ \pi \Rightarrow (h_1 \circ \pi) \circ \gamma = (h_2 \circ \pi) \circ \gamma \\ &\Rightarrow h_1 \circ (\pi \circ \gamma) = h_2 \circ (\pi \circ \gamma) \\ &\Rightarrow h_1 = h_1 \circ \mathrm{id}_B = h_2 \circ \mathrm{id}_B = h_2. \end{aligned}$$

(iii)⇒(i) Υποθέτουμε ότι η π είναι «εκ δεξιών διαγράψιμη». Εάν το B είναι μονοσύνολο, τότε η π είναι προδήλως επιρριπτική. Εάν το B περιέχει τουλάχιστον δύο στοιχεία y_1, y_2 με $y_1 \neq y_2$, τότε ορίζουμε τις απεικονίσεις

$$h_1(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_1, & \text{όταν } y \notin \mathrm{Im}(\pi), \end{cases} \quad h_2(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_2, & \text{όταν } y \notin \mathrm{Im}(\pi). \end{cases}$$

Προφανώς, $h_1(\pi(x)) = \pi(x) = h_2(\pi(x))$ για κάθε $x \in X$, οπότε

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

Εάν υπήρχε κάποιο $y \in B \smallsetminus \mathrm{Im}(\pi)$, τότε θα ίσχυε

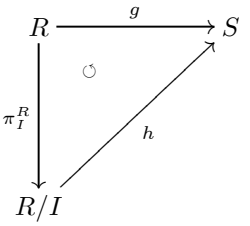
$$h_1(y) = h_2(y) \Longrightarrow y_1 = y_2,$$

ήτοι κάτι που θα αντέκειτο προς την υπόθεσή μας. Επομένως, $B = \mathrm{Im}(\pi)$. □

3.3.2 Θεώρημα. («Καθολική ιδιότητα πηλικοδακτυλίου») *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε για κάθε ομομορφισμό δακτυλίων $g : R \longrightarrow S$ για τον οποίον ισχύει $I \subseteq \mathrm{Ker}(g)$, η*

$$\boxed{h : R/I \longrightarrow S,\ \ a + I \longmapsto h(a + I) := g(a),\ \forall a \in R,}$$

είναι καλώς ορισμένη απεικόνιση και αποτελεί έναν ομομορφισμό δακτυλίων. Αυτός είναι ο μόνος ομομορφισμός από τον πηλικοδακτύλιο R/I στον δακτύλιο S που καθιστά το διάγραμμα



μεταθετικό (ήτοι $h \circ \pi_I^R = g$). Επιπροσθέτως, ισχύουν τα ακόλουθα:

(i) *Ο h είναι μονομορφισμός $\Longleftrightarrow I = \mathrm{Ker}(g)$.*

(ii) *Ο h είναι επιμορφισμός $\Longleftrightarrow$ ο g είναι επιμορφισμός.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς η h είναι καλώς ορισμένη απεικόνιση, διότι εάν έχουμε $a + I = b + I$, για κάποια $a, b \in R$, τότε

$$a - b \in I \subseteq \ \mathrm{Ker}\,(g) \Longrightarrow g(a - b) = g(a) - g(b) = 0_{R'} \Longrightarrow g(a) = g(b).$$

Επίσης, $h \circ \pi_I^R = g$, καθότι ισχύει

$$h\left(\pi_I^R(a)\right) = h(a + I) = g(a),\ \ \forall a \in R.$$

Το ότι η h είναι και ομομορφισμός δακτυλίων συνάγεται από τις ακόλουθες ισότητες:

$$\begin{cases} h((a + I) + (b + I)) = h((a + b) + I) = g(a + b) \\ = g(a) + g(b) = h(a + I) + h(b + I), \\ h((a + I)(b + I)) = h(ab + I) = g(ab) \\ = g(a)g(b) = h(a + I)\,h(b + I),\ \forall (a, b) \in R \times R. \end{cases}$$

Ο ομομορφισμός h είναι ο μόνος ομομορφισμός από τον R/I στον S που καθιστά το ως άνω διάγραμμα μεταθετικό. Πράγματι· εάν $h' : R/I \longrightarrow S$ είναι *τυχών* ομομορφισμός δακτυλίων με $h' \circ \pi_I^R = g$, τότε (σύμφωνα με τη συνεπαγωγή (i)⇒(iii) τού λήμματος 3.3.1)

$$h \circ \pi_I^R = h' \circ \pi_I^R \Longrightarrow h = h'.$$

(i) Υποθέτουμε ότι ο h είναι μονομορφισμός. Έστω τυχόν $a \in \mathrm{Ker}(g)$. Τότε

$$h\,(a+I) = g(a) = 0_S = h\left(0_{R/I}\right) = h\,(I) \underset{[h\ \text{ένριψη}]}{\Longrightarrow} a + I = I \Longrightarrow a \in I.$$

Άρα $\mathrm{Ker}(g) \subseteq I$. Κι επειδή (εξ υποθέσεως) $I \subseteq \mathrm{Ker}(g)$, έχουμε $\mathrm{Ker}(g) = I$.
Και αντιστρόφως· εάν υποθέσουμε ότι $\mathrm{Ker}(g) = I$, αρκεί να δείξουμε (επί τη βάσει τής προτάσεως 3.1.16) ότι $\mathrm{Ker}(h) = \{0_{R/I}\}$. Έστω λοιπόν τυχόν $a + I \in \mathrm{Ker}(h)$. Τότε

$$g(a) = h\,(a+I) = 0_S \Longrightarrow a \in \mathrm{Ker}\,(g) = I \Longrightarrow a + I = I = 0_{R/I},$$

απ' όπου έπεται ότι πράγματι $\mathrm{Ker}(h) = \{0_{R/I}\}$.
(ii) Εάν ο h είναι επιμορφισμός, τότε και ο $g = h \circ \pi_I^R$ είναι επιμορφισμός (ως σύνθεση δύο επιμορφισμών). Και αντιστρόφως· εάν ο $g = h \circ \pi_I^R$ είναι επιμορφισμός και $s \in S$, τότε υπάρχει κάποιο $r \in R$, τέτοιο ώστε να ισχύει $g(r) = s$. Άρα το $\pi_I^R(r)$ απεικονίζεται μέσω τής h στο s και ο h είναι επιμορφισμός. □

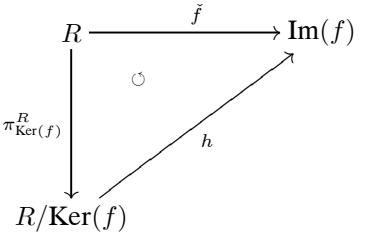
3.3.3 Πρώτο Θεώρημα Ισομορφισμών. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε*

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

Συγκεκριμένα, η απεικόνιση

$$\begin{aligned} h : R/\mathrm{Ker}(f) &\longrightarrow \mathrm{Im}\,(f) = f\,(R) \\ a + \mathrm{Ker}(f) &\longmapsto h(a + \mathrm{Ker}(f)) := f\,(a)\,, \end{aligned}$$

είναι (ο μόνος) ισομορφισμός δακτυλίων που καθιστά το διάγραμμα



μεταθετικό, όπου $\check{f}$ ο επιμορφισμός ο επαγόμενος μέσω τού f (βλ. 3.1.3 (viii)).

ΑΠΟΔΕΙΞΗ. Εφαρμόζουμε το θεώρημα 3.3.2 για το ιδεώδες $I := \mathrm{Ker}(f)$ τού R και για τον επιμορφισμό $g := \check{f}$. (Εν προκειμένω, η προϋποτεθείσα συνθήκη αυτού τού θεωρήματος ικανοποιείται, διότι $\mathrm{Ker}(f) = \mathrm{Ker}(\check{f})$.) Μάλιστα, ο κατασκευαζόμενος ομομορφισμός h είναι μονομορφισμός. Από την άλλη μεριά, η απεικόνιση h είναι, συν τοις άλλοις, και επιρριπτική, καθόσον για κάθε $s \in \mathrm{Im}(f)$ υπάρχει κάποιο $r \in R$ με $s = \check{f}(r) = f(r)$, οπότε $h(r + \mathrm{Ker}(f)) = s$. □

3.3.4 Παραδείγματα. (i) Έστω $m \in \mathbb{N}$ και έστω f ο επιμορφισμός δακτυλίων

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \;\; n \longmapsto [n]_m \,, \;\; \forall n \in \mathbb{Z}.$$

Τότε

$$\begin{aligned} \text{Ker}\,(f) &= \{ r \in \mathbb{Z} \mid \; f(r) = [0]_m \} = \{ r \in \mathbb{Z} \mid [r]_m = [0]_m \} \\ &= \{ r \in \mathbb{Z} \mid r = km, \; k \in \mathbb{Z} \} = \{ km \mid k \in \mathbb{Z} \} = m\mathbb{Z}, \end{aligned}$$

και, σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.3, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Εξάλλου, επειδή $m\mathbb{Z} = -m\mathbb{Z}$ για κάθε $m \in \mathbb{Z} \setminus \{0\}$, έχουμε γενικότερα

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|}, \; \forall m \in \mathbb{Z} \setminus \{0\}.} \tag{3.7}$$

(ii) Έστω R ο υποδακτύλιος τού $\text{Mat}_{2\times 2}\,(\mathbb{R})$ ο οριζόμενος ως εξής:

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\},$$

και έστω f η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{R}, \; \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \longmapsto a.$$

Τότε -όπως κανείς μπορεί εύκολα να ελέγξει- η f είναι ομομορφισμός δακτυλίων, οπότε, δυνάμει τού 1ου θεωρήματος ισομορφισμών 3.3.3,

$$\boxed{R/I \cong \mathbb{R},}$$

όπου

$$I = \text{Ker}\,(f) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}.$$

(iii) Έστω R ο υποδακτύλιος τού σώματος $\mathbb{Q}$ των ρητών αριθμών ο οριζόμενος ως εξής:

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

Η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{Z}_2, \;\; \tfrac{a}{b} \longmapsto f(\tfrac{a}{b}) := \begin{cases} [0]_2 \,, & \text{όταν } a \equiv 0 (\text{mod}\, 2), \\ [1]_2 \,, & \text{όταν } a \equiv 1 (\text{mod}\, 2), \end{cases}$$

είναι ομομορφισμός δακτυλίων και (βάσει τού θεωρήματος 3.3.3)

$$\boxed{R/\left\{ \tfrac{a}{b} \in R \middle|\; a \equiv 0 (\text{mod}\, 2) \right\} \cong \mathbb{Z}_2.}$$

(iv) Ο επιμορφισμός δακτυλίων

$$\mathbb{Z}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto a_0 \in \mathbb{Z}$$

έχει ως πυρήνα του το κύριο ιδεώδες

$$\left\{ \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \;\middle|\; a_0 = 0 \right\} = \langle \mathsf{X} \rangle ,$$

οπότε

$$\boxed{\mathbb{Z}[\mathsf{X}]/\langle \mathsf{X} \rangle \cong \mathbb{Z}.}$$

Επί τη βάσει των (i) και (iii) τού πορίσματος 3.1.11, τού θεωρήματος 2.6.4 και τού πορίσματος 2.6.5 το $\langle \mathsf{X} \rangle$ είναι πρώτο, μη μεγιστικό ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$.

3.3.5 Θεώρημα. (Μεταφορά ομομορφισμού σε «επίπεδο πηλικοδακτυλίων») *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Εάν I είναι ένα ιδεώδες τού R και J ένα ιδεώδες τού S,τότε οι εξής συνθήκες είναι ισοδύναμες*:

(i) *Υφίσταται ένας και μόνον ομομορφισμός $f^{\pi\eta\lambda.} : R/I \longrightarrow S/J$ ο οποίος καθιστά το διάγραμμα*

$$\begin{array}{ccc} R & \xrightarrow{\;f\;} & S \\ {\scriptstyle \pi_I^R}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \pi_J^S} \\ R/I & \xrightarrow[f^{\pi\eta\lambda.}]{} & S/J \end{array}$$

μεταθετικό, ήτοι ο «κανονιστικός» ομομορφισμός ο επαγόμενος από τον f που ορίζεται από τον τύπο

$$\boxed{f^{\pi\eta\lambda.}(r + I) := f(r) + J,\ \forall r \in R.}$$

(ii) $f(I) \subseteq J$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα ακόλουθα:

(a) *Ο $f^{\pi\eta\lambda.}$ είναι μονομορφισμός $\iff I = f^{-1}(J)$.*

(b) *Ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός $\iff \mathrm{Im}(f) + J = S$.*

ΑΠΟΔΕΙΞΗ. Εφαρμόζουμε το θεώρημα 3.3.2 για τον ομομορφισμό $\pi_J^S \circ f$ (με τους $R, I, S/J$ στη θέση των εκεί παρατεθέντων R, I και S, αντιστοίχως, και με τον $\pi_J^S \circ f$ στη θέση τού εκεί παρατεθέντος ομομορφισμού f). Σημειωτέον ότι

$$\mathrm{Ker}(\pi_J^S \circ f) = \{ r \in R \,|\, f(r) + J = J \} = \{ r \in R \,|\, f(r) \in J \} = f^{-1}(J).$$

Εάν λοιπόν $(I =) \operatorname{Ker}(\pi_I^R) \subseteq \operatorname{Ker}(\pi_J^S \circ f)$, τότε $f(I) \subseteq f(f^{-1}(J)) \subseteq J$. Και αντιστρόφως· εάν $f(I) \subseteq J$, τότε

$$I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(J) = \operatorname{Ker}(\pi_J^S \circ f).$$

Άρα η ανωτέρω συνθήκη (ii) ισοδυναμεί, εν προκειμένω, με τη συνθήκη τη δοθείσα στο θεώρημα 3.3.2. Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b) για τον ομομορφισμό $f^{\pi\eta\lambda.}$.

(a) Επειδή

$$\begin{aligned}\operatorname{Ker}(f^{\pi\eta\lambda.}) &= \{r + I \in R/I \,|\, f(r) + J = J\} = \{r + I \in R/I \,|\, f(r) \in J\} \\ &= \{r + I \in R/I \,|\, r \in f^{-1}(J)\} = f^{-1}(J)/I\end{aligned}$$

ο $f^{\pi\eta\lambda.}$ (λόγω τής προτάσεως 3.1.16) είναι μονομορφισμός $\iff I = f^{-1}(J)$.

(b) Επειδή $\operatorname{Im}(f^{\pi\eta\lambda.}) = \{f(r) + J \,|\, r \in R\}$, ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός εάν και μόνον εάν

$$(\forall s \in S)\,(\exists r \in R : f(r) + J = s + J) \Leftrightarrow (\forall s \in S)\,(\exists r \in R : f(r) - s \in J),$$

δηλαδή εάν και μόνον εάν $\operatorname{Im}(f) + J = S$. □

3.3.6 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και το I ένα ιδεώδες τού R, τέτοιο ώστε $\operatorname{Ker}(f) \subseteq I$. Τότε*

$$\boxed{R/I \cong S/f(I).}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 3.3.5. Προφανώς, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$\left.\begin{array}{r}f^{-1}(f(I)) = \operatorname{Ker}(f) + I \ \text{(βλ. 3.2.3 (iv))} \\ \operatorname{Ker}(f) \subseteq I \ \text{(εξ υποθέσεως)}\end{array}\right\} \Rightarrow I = f^{-1}(f(I)),$$

ο $f^{\pi\eta\lambda.}$ είναι *και* μονομορφισμός. □

3.3.7 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και το J ένα ιδεώδες τού S. Τότε*

$$\boxed{R/f^{-1}(J) \cong S/J.}$$

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 3.3.5. (Εν προκειμένω, ο κατασκευαζόμενος «κανονιστικός» ομομορφισμός $f^{\pi\eta\lambda.}$ είναι ισομορφισμός.) □

3.3.8 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής*:

(i) *Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{p})$ είναι ένα πρώτο ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{q})$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

ΑΠΟΔΕΙΞΗ. (i) Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου R που περιέχει τον πυρήνα τού f, τότε ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή και $R/\mathfrak{p} \cong S/f(\mathfrak{p})$ (λόγω τού θεωρήματος 2.6.4 και τού πορίσματος 3.3.6). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{p})$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 3.1.11). Αυτό σημαίνει ότι το $f(\mathfrak{p})$ οφείλει να είναι πρώτο ιδεώδες τού S (εκ νέου λόγω τού θεωρήματος 2.6.4).

(ii) Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου S, τότε ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή και $S/\mathfrak{q} \cong R/f^{-1}(\mathfrak{q})$ (λόγω τού θεωρήματος 2.6.4, τού πορίσματος 3.3.7 και τού (ii) τής προτάσεως 3.1.9). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι ακεραία περιοχή (βλ. το (i) τού πορίσματος 3.1.11). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{q})$ οφείλει να είναι πρώτο ιδεώδες τού δακτυλίου R (εκ νέου λόγω τού θεωρήματος 2.6.4). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{q}$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{q})$. □

3.3.9 Πόρισμα. (Θεώρημα αντιστοιχίσεως για πρώτα ιδεώδη.)
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα πρώτα φάσματα

$$\mathrm{Spec}(R) := \{\, \mathfrak{p} |\ \mathfrak{p} \text{ πρώτο ιδεώδες τού } R\}\,,\ \mathrm{Spec}(S) := \{\, \mathfrak{q} |\ \mathfrak{q} \text{ πρώτο ιδεώδες τού } S\}$$

των R και S (βλ. άσκηση **2-36**). *Εάν $\mathrm{Spec}(S) \neq \varnothing$, τότε η*

$$\begin{array}{ccc} \mathbf{V}(W) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq W\} & \longrightarrow & \mathrm{Spec}(S) \\ \mathfrak{p} & \longmapsto & f(\mathfrak{p}) \end{array} \tag{3.8}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \Longrightarrow f(\mathfrak{p}_1) \subsetneqq f(\mathfrak{p}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.8, για κάθε $\mathfrak{p} \in \mathbf{V}(W)$ έχουμε $f(\mathfrak{p}) \in \mathrm{Spec}(S)$ και για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ έχουμε $f^{-1}(\mathfrak{q}) \in \mathbf{V}(W)$. Επειδή $\mathfrak{p} = f^{-1}(f(\mathfrak{p}))$ για κάθε $\mathfrak{p} \in \mathbf{V}(W)$ και $\mathfrak{q} = f(f^{-1}(\mathfrak{q}))$ για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ (βλ. απόδειξη τού θεωρήματος 3.2.4), η (3.8) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός $\alpha|_{\mathbf{V}(W)}$ τής α τής ορισθείσας στο θεώρημα 3.2.4 επί τού $\mathbf{V}(W)$). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.4. □

3.3.10 Σημείωση. Εάν ο $f : R \longrightarrow S$ ένας ομομορφισμός (όχι κατ' ανάγκην επιμορφισμός!) μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, τότε

$$f^{-1}(\mathfrak{q}) \in \text{Spec}(R), \ \ \forall \mathfrak{q} \in \text{Spec}(S),$$

οπότε, υπό την προϋπόθεση ότι $\text{Spec}(S) \neq \varnothing$, ο f επάγει μια «κανονιστική» απεικόνιση (σε επίπεδο πρώτων φασμάτων):

$$\text{Spec}(S) \ni \mathfrak{q} \longmapsto f^{-1}(\mathfrak{q}) \in \text{Spec}(R).$$

Πράγματι· η αντίστροφη εικόνα $f^{-1}(\mathfrak{q})$ οιουδήποτε $\mathfrak{q} \in \text{Spec}(S)$ είναι ένα ιδεώδες τού R (βλ. 3.2.1 (ii)), ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή (βλ. θεώρημα 2.6.4) και η εφαρμογή τού 1ου θεωρήματος ισομορφισμών 3.3.3 για τη σύνθεση $\pi^S_{\mathfrak{q}} \circ f$ των ομομορφισμών

$$R \xrightarrow{f} S \xrightarrow{\pi^S_{\mathfrak{q}}} S/\mathfrak{q}$$

δίδει τον ισομορφισμό

$$R/\text{Ker}(\pi^S_{\mathfrak{q}} \circ f) \cong \text{Im}(\pi^S_{\mathfrak{q}} \circ f) \subseteq S/\mathfrak{q}.$$

Επειδή (σύμφωνα με το (iii) τής προτάσεως 3.1.5) η εικόνα $\text{Im}(\pi^S_{\mathfrak{q}} \circ f)$ είναι ένας υποδακτύλιος τής ακεραίας περιοχής $S/\mathfrak{q}$ και

$$1_{S/\mathfrak{q}} = 1_S + \mathfrak{q} = \pi^S_{\mathfrak{q}}(1_S) = \pi^S_{\mathfrak{q}}(f(1_R)) = (\pi^S_{\mathfrak{q}} \circ f)(1_R) = 1_{\text{Im}(\pi^S_{\mathfrak{q}} \circ f)}$$

(βλ. 3.1.5 (v)), η πρόταση 1.2.20 μας πληροφορεί ότι η $\text{Im}(\pi^S_{\mathfrak{q}} \circ f)$ είναι ακεραία περιοχή, οπότε και ο πηλικοδακτύλιος $R/\text{Ker}(\pi^S_{\mathfrak{q}} \circ f)$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 3.1.11). Επιπροσθέτως, επειδή

$$\begin{aligned} \text{Ker}(\pi^S_{\mathfrak{q}} \circ f) &= \left\{ r \in R \mid \pi^S_{\mathfrak{q}}(f(r)) = 0_{S/\mathfrak{q}} \right\} \\ &= \left\{ r \in R \mid f(r) + \mathfrak{q} = \mathfrak{q} \right\} \\ &= \left\{ r \in R \mid f(r) \in \mathfrak{q} \right\} = f^{-1}(\mathfrak{q}), \end{aligned}$$

ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι μια ακεραία περιοχή, οπότε έχουμε κατ' ανάγκην $f^{-1}(\mathfrak{q}) \in \text{Spec}(R)$ (βλ. θεώρημα 2.6.4).

3.3.11 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε πρώτο ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{p}/I$, όπου $\mathfrak{p}$ κάποιο (μονοσημάντως ορισμένο) πρώτο ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα πορίσματα 3.3.9 και 3.2.5. □

3.3.12 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής*:

(i) *Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{m}')$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

ΑΠΟΔΕΙΞΗ. (i) Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα και $R/\mathfrak{m} \cong S/f(\mathfrak{m})$ (λόγω των πορισμάτων 2.6.5 και 3.3.6). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{m})$ είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.11). Αυτό σημαίνει ότι το $f(\mathfrak{m})$ οφείλει να είναι μεγιστικό ιδεώδες τού S (εκ νέου λόγω τού πορίσματος 2.6.5).

(ii) Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε ο πηλικοδακτύλιος $S/\mathfrak{m}'$ είναι σώμα και $S/\mathfrak{m}' \cong R/f^{-1}(\mathfrak{m}')$ (λόγω των πορισμάτων 2.6.5 και 3.3.6, και τού (ii) τής προτάσεως 3.1.9). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{m}')$ είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.11). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{m}')$ οφείλει να είναι μεγιστικό ιδεώδες τού R (εκ νέου λόγω τού πορίσματος 2.6.5). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{m}'$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{m}')$. □

Εν συνεχεία, παραθέτουμε ένα πόρισμα ανάλογο τού 3.3.9 *για μεγιστικά ιδεώδη*.

3.3.13 Πόρισμα. (Θεώρημα αντιστοιχίσεως για μεγιστικά ιδεώδη.)
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα ***μεγιστικά φάσματα***

$$\text{Max-Spec}(R) := \left\{ \mathfrak{m} \;\middle|\; \begin{array}{c} \mathfrak{m} \text{ μεγιστικό} \\ \text{ιδεώδες τού } R \end{array} \right\}, \quad \text{Max-Spec}(S) := \left\{ \mathfrak{n} \;\middle|\; \begin{array}{c} \mathfrak{n} \text{ μεγιστικό} \\ \text{ιδεώδες τού } S \end{array} \right\}$$

των R και S. Εάν ο S είναι μη τετριμμένος, τότε η

$$\boxed{\begin{array}{ccc} \{\mathfrak{m} \in \text{Max-Spec}(R) \,|\, \mathfrak{m} \supseteq W\} & \longrightarrow & \text{Max-Spec}(S) \\ \mathfrak{m} & \longmapsto & f(\mathfrak{m}) \end{array}} \tag{3.9}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{m}_1 \subsetneqq \mathfrak{m}_2 \Longrightarrow f(\mathfrak{m}_1) \subsetneqq f(\mathfrak{m}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.12, η εικόνα $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού δακτυλίου S για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και το $f^{-1}(\mathfrak{m}')$ είναι μεγιστικό ιδεώδες τού R περιέχον τον W για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού S. Επειδή $\mathfrak{m} = f^{-1}(f(\mathfrak{m}))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και $\mathfrak{m}' = f(f^{-1}(\mathfrak{m}'))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού S (βλ. απόδειξη τού θεωρήματος 3.2.4), η (3.9) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής,

ο περιορισμός τής α τής ορισθείσας στο θεώρημα 3.2.4 επί τού συνόλου των μεγιστικών ιδεωδών τού R που περιέχουν τον W). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.4. □

3.3.14 Σημείωση. Έστω $f : R \longrightarrow S$ ένας ομομορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$. Εάν ο f δεν είναι επιμορφισμός, τότε, σε αντίθεση με ό,τι συμβαίνει στην περίπτωση θεωρήσεως αντιστρόφων εικόνων πρώτων ιδεωδών (βλ. 3.3.10), η αντίστροφη εικόνα ενός μεγιστικού ιδεώδους τού S μέσω τού f δεν είναι κατ' ανάγκην μεγιστικό ιδεώδες τού R. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, παρατηρούμε ότι η $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}$ είναι μονομορφισμός, δεν είναι επιμορφισμός, $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}(1) = 1$, το τετριμμένο ιδεώδες $\{0\}$ τού $\mathbb{Q}$ είναι μεγιστικό (βλ. πόρισμα 2.1.11), αλλά η αντίστροφη εικόνα $\mathrm{in}^{-1}_{\mathbb{Z},\mathbb{Q}}(\{0\}) = \{0\}$ τού $\{0\}$ είναι το τετριμμένο ιδεώδες τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών που *δεν είναι μεγιστικό ιδεώδες* (βλ. 2.5.23 (i)).

3.3.15 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε μεγιστικό ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{m}/I$, όπου $\mathfrak{m}$ κάποιο (μονοσημάντως ορισμένο) μεγιστικό ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα πορίσματα 3.3.13 και 3.2.5. □

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

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

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

(iii) *το I είναι ένα ιδεώδες τού $S + I$ και*

(iv) *υφίσταται ισομορφισμός δακτυλίων*

$$\boxed{S/(S \cap I) \cong (S + I)/I.}$$

ΑΠΟΔΕΙΞΗ. (i) Επειδή το I είναι ένα ιδεώδες τού R, έχουμε

$$\{0_S\} = \{0_R\} \subseteq S \cap I \subseteq S.$$

Επίσης, το $S \cap I$ αποτελεί προσθετική υποομάδα τής (αβελιανής) ομάδας $(S, +)$. Έστω τώρα τυχόν $a \in S \cap I$. Προφανώς, $a \in S$ και $a \in I$. Επειδή $a \in S$ και ο S είναι υποδακτύλιος τού R, ισχύει

$$sa \in S,\ \ as \in S,\ \forall s \in S,$$

λόγω τής κλειστότητας τής πράξεως τού πολλαπλασιασμού εντός τού S. Από την άλλη μεριά, επειδή το I είναι ιδεώδες τού R,

$$sa \in I,\ \ as \in I.$$

Επομένως, $sa, as \in S \cap I$ για κάθε $s \in S$ και κάθε $a \in S \cap I$. Εξ αυτών έπεται ότι το $S \cap I$ είναι ένα ιδεώδες τού S.

(ii) Εάν $s \in S$, τότε προφανώς $s + 0_R \in S + I$, αφού $0_R \in I$. Άρα $S \subseteq S + I$. Εν συνεχεία, ας υποθέσουμε ότι $x_1, x_2 \in S + I$. Τα x_1, x_2 γράφονται ως $x_1 = s_1 + a_1$ και $x_2 = s_2 + a_2$, για κάποια $s_1, s_2 \in S$ και $a_1, a_2 \in I$. Επομένως,

$$\left.\begin{aligned} x_1x_2 = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2, \\ s_1s_2 \in S, \\ s_1a_2 + a_1s_2 + a_1a_2 \in I \end{aligned}\right\} \Longrightarrow x_1x_2 \in S + I,$$

και

$$\left.\begin{aligned} x_1 - x_2 = (s_1 - s_2) + (a_1 - a_2)\,, \\ s_1 - s_2 \in S, \\ a_1 - a_2 \in I \end{aligned}\right\} \Longrightarrow x_1 - x_2 \in S + I.$$

Άρα τελικώς το $S + I$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$.

(iii) Έστω ότι $a, b \in I$ και $x = s + c \in S + I$, όπου $s \in S$ και $c \in I$. Τότε ο ισχυρισμός είναι αληθής λόγω τής συνεπαγωγής:

$$\left.\begin{aligned} a - b \in I \quad (\text{διότι το } I \text{ είναι ιδεώδες τού } R) \\ sa \in I \quad (\text{διότι } s \in R \text{ και το } I \text{ είναι ιδεώδες τού } R) \\ ca \in I \quad (\text{διότι το } I \text{ είναι υποδακτύλιος τού } R) \end{aligned}\right\} \Longrightarrow a - b,\ \ xa \in I.$$

(iv) Έστω f η απεικόνιση

$$f : S \longrightarrow (S + I)/I,\ \ s \longmapsto s + I,\ \ \forall s \in S.$$

Προφανώς, $f = \pi_I^{S+I} \circ j$, όπου $\pi_I^{S+I} : S + I \longrightarrow (S + I)/I$ ο επιμορφισμός κλάσεων υπολοίπων και $j : S \longrightarrow S + I$ η συνήθης ένθεση $s \longmapsto s\,(+0_R)$. Κατά το 1ο θεώρημα ισομορφισμών 3.3.3, $S/\mathrm{Ker}(f) \cong f(S)$. Θα αποδείξουμε εν πρώτοις ότι $\mathrm{Ker}(f) = S \cap I$. Έστω λοιπόν τυχόν $s \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{aligned} f(s) = s + I = 0_R + I \Longrightarrow s \in I \\ s \in S \end{aligned}\right\} \Longrightarrow s \in S \cap I.$$

Και αντιστρόφως· εάν $s \in S \cap I$, τότε $f(s) = s + I = 0_R + I = I \Longrightarrow s \in \mathrm{Ker}(f)$. Άρα πράγματι $\mathrm{Ker}(f) = S \cap I$. Ως εκ τούτου, αρκεί να αποδειχθεί η ισότητα: $f(S) = (S + I)/I$ (ήτοι ότι η f είναι επιρριπτική). Έστω τυχόν $b + I \in (S + I)/I$. Τότε $b = s + a$, για κάποια $s \in S$ και $a \in I$. Επομένως,

$$I \ni (s + a) - s = a \Longrightarrow f(s) = s + I = s + a + I = b + I,$$

πράγμα που επιβεβαιώνει την επιρριπτικότητα τής f. □

3.3.17 Πόρισμα. *Έστω ότι ο R είναι ένας δακτύλιος και τα I, J δύο ιδεώδη του. Τότε υφίστανται ισομορφισμοί*:

$$\boxed{I/\left(I\cap J\right)\cong\left(I+J\right)/J}$$

και

$$\boxed{\left(I+J\right)/\left(I\cap J\right)\cong\left(\left(I+J\right)/I\right)\times\left(\left(I+J\right)/J\right)\cong\left(J/\left(I\cap J\right)\right)\times\left(I/\left(I\cap J\right)\right).}$$

ΑΠΟΔΕΙΞΗ. Ο πρώτος ισομορφισμός είναι άμεσος δυνάμει τού 2ου θεωρήματος ισομορφισμών 3.3.16. Για την απόδειξη των άλλων δύο ισομορφισμών ορίζουμε την

$$f:I+J\longrightarrow\left(\left(I+J\right)/I\right)\times\left(\left(I+J\right)/J\right),\ \ a\longmapsto\left(a+I,a+J\right),\ \forall a\in I+J.$$

Είναι εύκολος ο έλεγχος τού ότι η f αποτελεί ομομομορφισμό δακτυλίων. Ο πυρήνας της ισούται προφανώς με

$$\begin{aligned}\mathrm{Ker}(f) &= \left\{a\in I+J\mid f(a)=0_{((I+J)/I)\times((I+J)/J)}\right\}\\ &= \left\{a\in I+J\mid (a+I,a+J)=(I,J)\right\}\\ &= \left\{a\in I+J\mid a\in I,\ a\in J\right\}=I\cap J.\end{aligned}$$

Εν συνεχεία, θα δείξουμε ότι η f είναι επιρριπτική. Έστω τυχόν

$$(a+I,b+J)\in\left(\left(I+J\right)/I\right)\times\left(\left(I+J\right)/J\right).$$

Τότε τα a, b γράφονται ως αθροίσματα

$$a=u+v,\ \ b=w+z,$$

για κατάλληλα $u,w\in I$ και $v,z\in J$. Κατά συνέπειαν,

$$\begin{aligned}f(v) &= (v+I,v+J)=(v+I,0_{I+J}+J),\\ f(w) &= (w+I,w+J)=(0_{I+J}+I,w+J),\end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$f(v+w)=f(v)+f(w)=(v+I,w+J)=(u+v+I,w+z+J)=(a+I,b+J),$$

δηλαδή ότι η f είναι επιμορφισμός με $\mathrm{Ker}(f)=I\cap J$. Αρκεί η εφαρμογή τού 1ου θεωρήματος ισομορφισμών. Τέλος, ο τρίτος -κατά σειράν- ισομορφισμός έπεται κατόπιν απευθείας εφαρμογής τού 2ου θεωρήματος ισομορφισμών 3.3.16 σε αμφότερους τους παράγοντες τού μετέχοντος καρτεσιανού γινομένου δακτυλίων. □

3.3.18 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle m \rangle$, $J = \langle n \rangle$, όπου $m, n \in \mathbb{Z} \setminus \{0\}$, τότε, λαμβάνοντας υπ' όψιν τα όσα αποδείξαμε στα 2.4.13 (i), (ii), οι ισομορφισμοί οι θεσπισθέντες μέσω τού πορίσματος 3.3.17 γράφονται υπό τη μορφή:

$$\langle m \rangle \,/\, \langle \text{εκπ}(m,n) \rangle \cong \langle \text{μκδ}(m,n) \rangle \,/\, \langle n \rangle$$

και, αντιστοίχως,

$$\begin{aligned} \langle \text{μκδ}(m,n) \rangle \,/\, \langle \text{εκπ}(m,n) \rangle &\cong (\langle \text{μκδ}(m,n) \rangle \,/\, \langle m \rangle) \times (\langle \text{μκδ}(m,n) \rangle \,/\, \langle n \rangle) \\ &\cong (\langle n \rangle \,/\, \langle \text{εκπ}(m,n) \rangle) \times (\langle m \rangle \,/\, \langle \text{εκπ}(m,n) \rangle)\,. \end{aligned}$$

3.3.19 Ορισμός. Εάν τα I, J είναι δυο ιδεώδη ενός δακτυλίου R και ισχύει η ισότητα $R = I + J$, τότε λέμε ότι τα I και J είναι **συμπρώτα**.

3.3.20 Πόρισμα. *Εάν τα I, J είναι συμπρώτα ιδεώδη ενός δακτυλίου R, τότε*

$$\boxed{R/\,(I \cap J) \cong (R/I) \times (R/J)\,.}$$

3.3.21 Τρίτο Θεώρημα Ισομορφισμών. *Εάν ο R είναι ένας δακτύλιος και τα I, J γνήσια ιδεώδη τού R με $I \subseteq J$, τότε έχουμε*

$$\boxed{R/J \cong (R/I)\ /\,(J/I).}$$

ΑΠΟΔΕΙΞΗ. Έστω f η απεικόνιση

$$f : R \longrightarrow (R/I)\ /\,(J/I)\ ,\ \ a \longmapsto (a+I) + (J/I),\ \forall a \in R.$$

Επειδή $f = \pi^{R/I}_{J/I} \circ \pi^R_I$, όπου $\pi^R_I : R \longrightarrow (R/I)$ και $\pi^{R/I}_{J/I} : R/I \longrightarrow (R/I)\ /\,(J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.3,

$$R/\text{Ker}\,(f) \cong (R/I)\ /\,(J/I)\ .$$

Όμως

$$\begin{aligned} \text{Ker}(f) &= \left\{ a \in R \mid\ f(a) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \left\{ a \in R \mid\ \pi^{R/I}_{J/I}(\pi^R_I(a)) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \left\{ a \in R \mid\ \pi^{R/I}_{J/I}(a+I) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \left\{ a \in R \mid\ a + I \in \text{Ker}(\pi^{R/I}_{J/I}) \right\} \\ &= \{ a \in R \mid\ a + I \in (J/I) \} = J, \end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

3.3.22 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle 12\rangle = 12\mathbb{Z} \subsetneqq J = \langle 3\rangle = 3\mathbb{Z}$, τότε, επειδή το ιδεώδες $3\mathbb{Z}/12\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}/12\mathbb{Z}$ περιέχει εκείνες τις κλάσεις υπολοίπων τού $\mathbb{Z}/12\mathbb{Z}$, οι εκπρόσωποι των οποίων ανήκουν στο $J = 3\mathbb{Z}$, ήτοι είναι πολλαπλάσια τού 3, έχουμε $J/I = \{I,\ 3+I,\ 6+I,\ 9+I\}$ και

$$(\mathbb{Z}/I)\ /\,(J/I) = \{\,k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leq k \leq 11\}\,.$$

Σημειωτέον ότι υπάρχουν πολλαπλές εμφανίσεις μεταξύ αυτών των δώδεκα στοιχείων, καθότι

$$\begin{aligned}&(k_1 + I) - (k_2 + I) \in J/I \Longleftrightarrow (k_1 - k_2) + I \in J/I\\ &\Longleftrightarrow 3 \mid k_1 - k_2.\end{aligned}$$

Ως εκ τούτου, ο δακτύλιος $(\mathbb{Z}/I)\ /\,(J/I)$ συνίσταται από ακριβώς τρεις σαφώς διακεκριμένες κλάσεις ισοτιμίας:

$$(\mathbb{Z}/I)\ /\,(J/I) = \{\,k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leq k \leq 2\}\,.$$

Κατά το 1ο και το 3ο θεώρημα ισομορφισμών (βλ. 3.3.3 και 3.3.21),

$$\mathbb{Z}_3 = \{[0]_3\,, [1]_3\,, [2]_3\} \cong \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/I)\ /\,(J/I) = \{(J/I, 1 + (J/I), 2 + (J/I)\}.$$

3.4 ΕΦΑΡΜΟΓΗ: ΛΥΣΕΙΣ ΣΥΣΤΗΜΑΤΩΝ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Στην ενότητα 3.3 παρετέθησαν ορισμένα πρώτα παραδείγματα εφαρμογής των θεωρημάτων ισομορφισμών δακτυλίων (βλ. 3.3.4, 3.3.18 και 3.3.22). Εδώ θα παρουσιασθεί μια επιπρόσθετη, αρκούντως σημαντική εφαρμογή *αριθμοθεωρητικής φύσεως* σχετιζόμενη με τον προσδιορισμό τού συνόλου των λύσεων συστημάτων πεπερασμένου πλήθους γραμμικών ισοτιμιών (με έναν άγνωστο). Το κύριο θεώρημα τής παρούσας ενότητας είναι το 3.4.10, το επονομαζόμενο *Κινέζικο θεώρημα* [3] ή *θεώρημα τού Νικομάχου τού Γερασηνού* [4], για το οποίο δίνουμε μια καθαρώς «δακτυλιοθεωρητική» απόδειξη (αν και στη γενίκευσή του 3.4.15 δεν παραλείπουμε και την παράθεση μιας πιο «στοιχειώδους» προσβάσεως).

[3] Παρότι στη βιβλιογραφία είναι γνωστό ως *Chinese remainder theorem,* πιθανολογείται πως οι Κινέζοι μαθηματικοί τού 3ου μ.Χ. αιώνα, οι οποίοι έδωσαν μια πρακτική μέθοδο επιλύσεως ενός συστήματος τριών γραμμικών ισοτιμιών, είχαν λάβει γνώση τού έργου τού Νικομάχου τού Γερασηνού, αφού το εν λόγω σύστημα περιέχει τους ίδιους αριθμούς με εκείνους τού Νικομάχου! Η πρώτη ολοκληρωμένη απόδειξη τού θεωρήματος 3.4.10 οφείλεται στον L. Euler, ενώ μια νεότερη απόδειξη ανακαλύφθηκε (μάλλον ανεξαρτήτως) από τον C.-F. Gauss περί το έτος 1801.

[4] Ο φιλόσοφος και μαθηματικός *Νικόμαχος ο Γερασηνός* (από τα Γέρασα, μια αρχαιοελληνική πόλη στην Παλαιστίνη, 30 μίλια νοτιοανατολικά τής λίμνης Τιβεριάδος, ιδρυθείσα από τον Μ. Αλέξανδρο) θα πρέπει -εξ όσων γνωρίζουμε- να έζησε σε κάποιο διάστημα μεταξύ τού μέσου τού 1ου και τού μέσου τού 2ου μ.Χ. αιώνα. Πέραν τής γνωστής του «Αριθμητικής Εισαγωγής» είχε συγγράψει και πολλά άλλα έργα, εκ των οποίων ελάχιστα τμήματα διεσώθησαν. Σε ένα όμως εξ αυτών παρατίθεται η λύση τού συστήματος των ισοτιμιών $x \equiv 2 (\mathrm{mod}\, 3)$, $x \equiv 3 (\mathrm{mod}\, 5)$ και $x \equiv 2 (\mathrm{mod}\, 7)$. (Για να την προσδιορίσετε, εφαρμόστε τό 3.4.10!)

► **Γραμμικές ισοτιμίες**. Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b δυο ακέραιοι αριθμοί. Κάθε ισοτιμία τής μορφής

$$\boxed{ax \equiv b(\mathrm{mod}\, m),} \tag{3.10}$$

με το x προσδιοριστέο εντός τού συνόλου των ακεραίων αριθμών, καλείται **γραμμική ισοτιμία** (με *άγνωστό της* τον x). Λέμε ότι ένας $x_0 \in \mathbb{Z}$ *πληροί* (ή *επαληθεύει*) την (3.10) όταν $ax_0 \equiv b(\mathrm{mod}\, m)$. Εν τοιαύτη περιπτώσει, *και οιοσδήποτε άλλος* εκπρόσωπος τής κλάσεως υπολοίπων $[x_0]_m$ τού x_0 επαληθεύει την (3.10). Πράγματι· εάν $y \in [x_0]_m$, τότε $[y]_m = [x_0]_m$, απ' όπου έπεται ότι $y \equiv x_0(\mathrm{mod}\, m)$, οπότε

$$ay \equiv ax_0 \equiv b(\mathrm{mod}\, m).$$

Ως εκ τούτου, όταν ομιλούμε για μια **λύση** $x_0 \in \mathbb{Z}$ **τής** (3.10) **κατά μόδιο** m, εννοούμε ολόκληρη[5] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (3.10). Επίσης, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα και συναντούμε μια λύση $[x_0]_m$, προτιμούμε να παραθέτουμε τον *μοναδικό* εκπρόσωπο x_0' τής κλάσεως υπολοίπων $[x_0]_m$ ο οποίος ανήκει στο σύνολο $\{0, 1, \ldots, m-1\}$, ήτοι να καταφεύγουμε σε *αναγωγή* τού x_0 κατά μόδιο m κατόπιν διαιρέσεώς του διά τού m.

Σημειωτέον ότι υπάρχουν γραμμικές ισοτιμίες οι οποίες δεν δέχονται καμία ακεραία λύση, όπως π.χ. η $2x \equiv 3(\mathrm{mod}\, 4)$, αφού για κάθε $k \in \mathbb{Z}$ ο ακέραιος $2k-3$ είναι περιττός και επομένως $4 \nmid 2k-3$. Η πρόταση που ακολουθεί μας γνωστοποιεί την ικανή και αναγκαία συνθήκη για την ύπαρξη ακεραίων λύσεων τής (3.10) και, επιπροσθέτως, περιγράφει τη μορφή όλων των δυνατών λύσεων.

3.4.1 Πρόταση. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (3.10) *διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν* $\mathrm{μκδ}\,(a, m) \mid b$. *Επιπροσθέτως, όταν* $\mathrm{μκδ}\,(a, m) \mid b$, *η ισοτιμία* (3.10) *διαθέτει ακριβώς* $\mathrm{μκδ}(a, m)$ *σαφώς διακεκριμένες λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής*

$$\boxed{x = x_0 + k\,\frac{m}{\mathrm{μκδ}\,(a, m)}, \quad k \in \{0, 1, \ldots, \mathrm{μκδ}\,(a, m) - 1\},} \tag{3.11}$$

όπου x_0 μια ειδική λύση τής (3.10).

ΑΠΟΔΕΙΞΗ. Εάν η (3.10) δέχεται μια λύση $x \in \mathbb{Z}$ κατά μόδιο m, τότε

$$ax \equiv b(\mathrm{mod}\ m) \Longrightarrow m \mid ax - b \Longrightarrow (\exists k \in \mathbb{Z} : b = ax - km)\,.$$

Επομένως,

$$\left.\begin{array}{r} \mathrm{μκδ}\,(a, m) \mid a \\ \mathrm{μκδ}\,(a, m) \mid m \end{array}\right\} \Longrightarrow \mathrm{μκδ}\,(a, m) \mid ax - km\ (= b).$$

[5] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (3.10) λογίζονται ως *διαφορετικές* όταν $x_1 \not\equiv x_2 (\mathrm{mod}\, m)$.

Και αντιστρόφως· εάν $\mu\kappa\delta(a,m) \mid b$, τότε $b = \mu\kappa\delta(a,m)\, b'$ για κάποιον $b' \in \mathbb{Z}$. Επειδή

$$\mu\kappa\delta\left(\tfrac{a}{\mu\kappa\delta(a,m)}, \tfrac{m}{\mu\kappa\delta(a,m)}\right) = 1 \Longrightarrow \left(\exists \kappa, \lambda \in \mathbb{Z} : \kappa \tfrac{a}{\mu\kappa\delta(a,m)} + \lambda \tfrac{m}{\mu\kappa\delta(a,m)} = 1\right),$$

λαμβάνουμε

$$b = \kappa \tfrac{ab}{\mu\kappa\delta(a,m)} + \lambda \tfrac{mb}{\mu\kappa\delta(a,m)} = a\,(\kappa b') + m\,(\lambda b') \Longrightarrow a\,(\kappa b') \equiv b (\mathrm{mod}\ m),$$

οπότε η κλάση ισοτιμίας τού $\kappa b'$ κατά μόδιο m είναι μια λύση τής (3.10).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (3.10). Προφανώς,

$$a\left(x_0 + k\frac{m}{\mu\kappa\delta\,(a,m)}\right) = ax_0 + \left(\frac{ak}{\mu\kappa\delta\,(a,m)}\right) m \equiv b (\mathrm{mod}\ m),$$

οπότε οι ακέραιοι (3.11) αποτελούν πράγματι λύσεις τής (3.10). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε ακεραίους αριθμούς $k, k' \in \{0, 1, \ldots, \mu\kappa\delta(a,m) - 1\}$ με $k \neq k'$, έχουμε

$$\left|\left(x_0 + \tfrac{mk}{\mu\kappa\delta(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\mu\kappa\delta(a,m)}\right)\right| = |k - k'|\ \tfrac{m}{\mu\kappa\delta(a,m)} < m,$$

αφού $|k - k'| < \mu\kappa\delta(a,m)$. Συνεπώς,

$$\begin{gathered} m \nmid \left(x_0 + \tfrac{mk}{\mu\kappa\delta(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\mu\kappa\delta(a,m)}\right) \\ \Downarrow \\ \left(x_0 + \tfrac{mk}{\mu\kappa\delta(a,m)}\right) \not\equiv \left(x_0 + \tfrac{mk'}{\mu\kappa\delta(a,m)}\right) (\mathrm{mod}\ m). \end{gathered}$$

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y \in \mathbb{Z}$ τής (3.10) είναι ισότιμη με κάποια εκ των (3.11) κατά μόδιο m. Επειδή

$$\left.\begin{aligned} ax_0 &\equiv b (\mathrm{mod}\ m) \\ ay &\equiv b (\mathrm{mod}\ m) \end{aligned}\right\} \Longrightarrow ax_0 \equiv ay (\mathrm{mod}\ m) \Longrightarrow m \mid a\,(y - x_0),$$

συμπεραίνουμε ότι

$$\left.\begin{aligned} \tfrac{m}{\mu\kappa\delta(a,m)} &\mid \tfrac{a}{\mu\kappa\delta(a,m)}\,(y - x_0) \\ \mu\kappa\delta\left(\tfrac{a}{\mu\kappa\delta(a,m)}, \tfrac{m}{\mu\kappa\delta(a,m)}\right) &= 1 \end{aligned}\right\} \Longrightarrow \begin{gathered} \tfrac{m}{\mu\kappa\delta(a,m)} \mid y - x_0 \\ \Downarrow \\ \left(\exists \nu \in \mathbb{Z} : y - x_0 = \tfrac{m\nu}{\mu\kappa\delta(a,m)}\right). \end{gathered}$$

Διαιρώντας τον ν διά τού $\mu\kappa\delta(a,m)$ λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z}^2$ με

$$\nu = \mu\kappa\delta\,(a,m)\, q + r, \quad 0 \leq r \leq \mu\kappa\delta\,(a,m) - 1.$$

Ως εκ τούτου,

$$y - x_0 = \frac{m(\text{μκδ}(a,m)q+r)}{\text{μκδ}(a,m)} = mq + \frac{rm}{\text{μκδ}(a,m)} \equiv \frac{rm}{\text{μκδ}(a,m)} (\text{mod } m),$$

οπότε $y \equiv x_0 + r\frac{m}{\text{μκδ}(a,m)} (\text{mod } m)$, $\forall r \in \{0, 1, \dots, \text{μκδ}(a,m) - 1\}$. □

3.4.2 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (3.10) *διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m εάν και μόνον εάν* μκδ $(a, m) = 1$.

3.4.3 Σημείωση. Όταν μκδ$(a, m) = 1$, ένας τρόπος υπολογισμού τής λύσεως x_0 κατά μόδιο m διασφαλίζεται μέσω τής προσφυγής μας στον κλασικό *ευκλείδειο αλγόριθμο* (ήτοι στον προσδιορισμό ενός ζεύγους $(x_0^*, y_0^*) \in \mathbb{Z}^2$ για το οποίο ισχύει $ax_0^* - my_0^* = 1$, ορίζοντας ως x_0 το $x_0 := bx_0^*$). Ένας άλλος τρόπος υπολογισμού τής λύσεως x_0 είναι δυνατός κατόπιν εφαρμογής *τού θεωρήματος τού Euler περί ισοτιμιών*. Σύμφωνα με αυτό, (λόγω τής συνθήκης μκδ$(a, m) = 1$) έχουμε

$$\boxed{a^{\phi(m)} \equiv 1(\text{mod } m),}$$

όπου ϕ η συνάρτηση φι τού Euler. Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\phi(m)-1}b,} \tag{3.12}$$

να εφαρμόσουμε τον γνωστό τύπο ευρέσεως τού $\phi(m)$ για τον δοθέντα φυσικό αριθμό m και να διενεργήσουμε αναγωγή κατά μόδιο m.

3.4.4 Παράδειγμα. Επειδή μκδ$(5, 24) = 1$, η γραμμική ισοτιμία $5x \equiv 3(\text{mod } 24)$ διαθέτει *ακριβώς μία* λύση x_0 κατά μόδιο m. Γράφοντας $24 = 2^3 \cdot 3$, διαπιστώνουμε άμεσα ότι $\phi(24) = (2^3 - 2^2)(3 - 1) = 8$. Κατά τον (3.12), μπορούμε να θέσουμε ως $x_0 := 5^7 \cdot 3 = 234\,375$. Επειδή $234\,375 = 9765 \cdot 24 + 15$, έχουμε $[x_0]_{24} = [15]_{24}$, οπότε $5 \cdot 15 \equiv 3(\text{mod } 24)$.

Η εύρεση των λύσεων τής γενικής γραμμικής ισοτιμίας (3.10) ανάγεται -κατ' ουσίαν- στην ειδική περίπτωση που περιγράψαμε στα 3.4.2 και 3.4.3, ως ακολούθως:

3.4.5 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, με* μκδ $(a, m) | b$, *η γραμμική ισοτιμία* (3.10) *διαθέτει* μκδ(a, m) *λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής* (3.11), *όπου x_0 η μοναδική λύση κατά μόδιο $\frac{m}{\text{μκδ}(a,m)}$ τής*

$$\left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) (\text{mod } \left(\tfrac{m}{\text{μκδ}(a,m)}\right)). \tag{3.13}$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $\widetilde{a} := \frac{a}{\text{μκδ}(a,m)}$, $\widetilde{b} := \frac{b}{\text{μκδ}(a,m)}$ και $\widetilde{m} := \frac{m}{\text{μκδ}(a,m)}$, έχουμε μκδ$(\widetilde{a}, \widetilde{m}) = 1$, καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} ax \equiv b \,(\text{mod } m) &\iff \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b} \,(\text{mod}\, \text{μκδ}\,(a,m)\,\widetilde{m}) \\ &\iff \widetilde{a}x \equiv \widetilde{b} \,(\text{mod } \widetilde{m}) \\ &\iff \left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) \,(\text{mod } \left(\tfrac{m}{\text{μκδ}(a,m)}\right)), \end{aligned}$$

διότι μκδ$(a,m) \neq 0$, οπότε η (3.13) ισοδυναμεί με την (3.10). □

3.4.6 Παράδειγμα. Η γραμμική ισοτιμία

$$6x \equiv 3 (\text{mod}\, 21)$$

διαθέτει μκδ$(6,21) = 3$ λύσεις κατά μόδιο 21 τής μορφής x_0, $x_0 + 7$, $x_0 + 14$, όπου σύμφωνα με το πόρισμα 3.4.5 το x_0 είναι η μοναδική λύση τής $2x \equiv 1 (\text{mod}\, 7)$ κατά μόδιο 7. Εφαρμόζοντας τον τύπο (3.12) θέτουμε

$$x_0 = 2^{\phi(7)-1} = 2^5 = 32 \equiv 4 (\text{mod}\, 7).$$

Άρα οι λύσεις τής αρχικής είναι οι $4, 11, 18$ κατά μόδιο 21.

► **Συστήματα γραμμικών ισοτιμιών**. Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \ldots, a_k,\ b_1, \ldots, b_k$, υπό ποίες συνθήκες είναι το σύστημα των γραμμικών ισοτιμιών

$$\left\{ \begin{array}{c} a_1 x \equiv b_1 \,(\text{mod } m_1) \\ \vdots \\ a_k x \equiv b_k \,(\text{mod } m_k) \end{array} \right\}$$

επιλύσιμο; Και πώς, πληρουμένων των εν λόγω συνθηκών, είναι δυνατόν να προσδιορισθεί επακριβώς το σύνολο λύσεων αυτού; Κατά την πορεία που θα ακολουθήσουμε προκειμένου να καταλήξουμε σε πλήρεις απαντήσεις σε αυτά τα ερωτήματα (μέσω τού θεωρηματος 3.4.16) θα χρησιμοποιήσουμε κατάλληλους *ισομορφισμούς δακτυλίων*.

3.4.7 Λήμμα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια, ώστε*

$$I_j + I_k = R,\ \forall\,(j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\ \ j \neq k,$$

τότε

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

ΑΠΟΔΕΙΞΗ. Θα κάνουμε χρήση μαθηματικής επαγωγής ως προς τον n. Για $n = 2$ ο ισχυρισμός είναι προφανώς αληθής. Υποθέτουμε λοιπόν ότι είναι αληθής και για κάποιον $n = l \geq 2$ και εξετάζουμε την περίπτωση όπου $n = l + 1$. Επειδή ο R είναι δακτύλιος με μοναδιαίο στοιχείο, έχουμε[6] $R = RR$. Κατά συνέπειαν, για κάθε $j \in \mathbb{N}$, $1 \leq j \leq l + 1$,

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

με τη δεύτερη ισότητα ισχύουσα λόγω επαγωγικής υποθέσεως και την επακόλουθη εγκλειστική σχέση απορρέουσα από την πρόταση 2.4.5 (ii). Επειδή όμως το δεξιό μέλος εμπεριέχεται στον R, έχουμε $R = I_j + \bigcap_{1 \leq k \leq l+1,\ k \neq j} I_k$. □

3.4.8 Θεώρημα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια ώστε*

$$I_j + I_k = R,\ \forall\, (j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\ \ j \neq k,$$

τότε έχουμε

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

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ. Για $n = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 3.3.20. Εάν υποτεθεί ότι $n \geq 3$ και ότι αυτός είναι αληθής για $n - 1$ όρους, τότε μέσω μαθηματικής επαγωγής και εφαρμογής τού λήμματος 3.4.7 (για $j = n$) λαμβάνουμε

$$\begin{aligned} R/\bigcap_{j=1}^{n} I_j = R/(\bigcap_{j=1}^{n-1} I_j \cap I_n) &\underset{3.3.20}{\cong} \left(R/\bigcap_{j=1}^{n-1} I_j \right) \times R/I_n \\ &\underset{(\text{επαγ. υπ.})}{\cong} (R/I_1) \times \cdots \times (R/I_n)\,. \end{aligned}$$

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ. Αυτή η απόδειξη είναι καθαρώς *κατασκευαστική*. Για κάθε $j \in \{1, \ldots, n\}$ ορίζουμε την απεικόνιση

$$f : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$$

$$r \longmapsto f(r) := (\pi^R_{I_1}(r), .., \pi^R_{I_n}(r)) = (r + I_1, .., r + I_n)\,.$$

Η f είναι προφανώς ομομορφισμός δακτυλίων και $\mathrm{Ker}(f) = \bigcap_{j=1}^{n} I_j$. Θα δείξουμε ότι η f είναι και *επιριπτική*. Έστω $\mathbf{y} = (y_1, \ldots, y_n) \in (R/I_1) \times \cdots \times (R/I_n)$.

[6] Για δακτύλιους χωρίς μοναδιαίο κάτι τέτοιο δεν ισχύει εν γένει! Επί παραδείγματι, $(2\mathbb{Z})\,(2\mathbb{Z}) \subsetneq (2\mathbb{Z})$.

Επειδή κάθε $\pi^R_{I_j}$ είναι επιρριπτική απεικόνιση, υπάρχει $x_j \in R$, τέτοιο ώστε $\pi^R_{I_j}(x_j) = y_j$. Κατά το λήμμα 3.4.7,

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

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

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

Συνεπώς,

$$\begin{aligned} f\left(\sum_{j=1}^n x_j v_j\right) &= \left(\pi^R_{I_1}(\sum_{j=1}^n x_j v_j), \dots, \pi^R_{I_n}(\sum_{j=1}^n x_j v_j)\right) \\ &= \left(\pi^R_{I_1}(x_1), \dots, \pi^R_{I_n}(x_n)\right) = \mathbf{y}, \end{aligned} \tag{3.14}$$

και η f είναι όντως επιρριπτική. Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3, ούτως ώστε να εισπράξουμε έναν «απτό» ισομορφισμό

$$\begin{aligned} R/\bigcap_{j=1}^n I_j &\xrightarrow{\ \cong\ } (R/I_1)\times\cdots\times(R/I_n) \\ r + \bigcap_{j=1}^n I_j &\longmapsto f(r) = (r + I_1, \dots, r + I_n) \end{aligned} \tag{3.15}$$

μεταξύ των δύο θεωρηθέντων πηλικοδακτυλίων. □

3.4.9 Πόρισμα. *Έστω n ένας φυσικός αριθμός ≥ 2 και έστω*

$$n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k},\ k \in \mathbb{N},$$

η κανονική παράσταση τού n ως γινομένου σαφώς διακεκριμένων πρώτων αριθμών $p_1, \dots, p_k$, υψωμένων σε κατάλληλες δυνάμεις $\nu_1, \dots, \nu_k \in \mathbb{N}$. Τότε έχουμε

$$\boxed{\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}/(p_1^{\nu_1}\mathbb{Z}) \times \cdots \times \mathbb{Z}/(p_k^{\nu_k}\mathbb{Z}).}$$

ΑΠΟΔΕΙΞΗ. Εάν $k = 1$, τούτο είναι προφανές. Έστω ότι $k \geq 2$ και ότι $I_j := p_j^{\nu_j}\mathbb{Z}$ για κάθε $j \in \{1,\dots,k\}$. Επειδή

$$\text{μκδ}(p_j^{\nu_j}, p_l^{\nu_l}) = 1,\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j,l \leq k,\ \ j \neq l,$$

υπάρχουν $\lambda, \mu \in \mathbb{Z}$, τέτοιοι ώστε $\lambda p_j^{\nu_j} + \mu p_l^{\nu_l} = 1$. Αυτό σημαίνει ότι για κάθε $x \in \mathbb{Z}$ έχουμε

$$x = x\lambda p_j^{\nu_j} + x\mu p_l^{\nu_l} \in I_j + I_l.$$

Άρα

$$I_j + I_l = \mathbb{Z},\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j,l \leq k,\ \ j \neq l.$$

Εν συνεχεία, θα αποδείξουμε την ισότητα

$$n\mathbb{Z} = \bigcap_{j=1}^{k} I_j.$$

Έστω τυχόν $x \in \langle n\rangle = n\mathbb{Z}$. Τότε $x = \lambda p_1^{\nu_1} p_2^{\nu_2} \cdots p_k^{\nu_k}$ για κάποιο $\lambda \in \mathbb{Z}$, οπότε

$$[x \in I_j,\ \ \forall j \in \{1,\ldots,k\}] \Longrightarrow x \in \bigcap_{j=1}^{k} I_j.$$

Και αντιστρόφως· εάν $x \in \bigcap\limits_{j=1}^{k} I_j$, τότε $x = \mu_1 p_1^{\nu_1} = \cdots = \mu_k p_k^{\nu_k}$ για κάποια $\mu_1,\ldots,\mu_k \in \mathbb{Z}$. Συνεπώς,

$$\left.\begin{array}{r} p_j^{\nu_j} \,|\, x,\quad \forall j \in \{1,\ldots,k\} \\ p_1,\ldots,p_k \\ \text{σαφώς διακεκριμένοι} \end{array}\right\} \Longrightarrow n = \prod_{j=1}^{k} p_j^{\nu_j} \,\Big|\, x \Longrightarrow x \in \langle n\rangle = n\mathbb{Z}.$$

Αρκεί λοιπόν να εφαρμόσουμε το θεώρημα 3.4.8. □

3.4.10 Πόρισμα. (Κινέζικο Θεώρημα ή Θεώρημα τού Νικομάχου τού Γερασηνού) *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1,\ldots,m_k$ και k ακεραίων αριθμών $b_1,\ldots,b_k$, για τους οποίους ισχύει*

$$\text{μκδ}\,(m_j,m_l) = 1,\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j,l \leq n,\ \ j \neq l,$$

το σύστημα των γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x \equiv b_1 (\mathrm{mod}\ m_1) \\ \vdots \\ x \equiv b_k (\mathrm{mod}\ m_k) \end{array}\right\} \tag{3.16}$$

είναι επιλύσιμο. Μάλιστα, εάν το x_0 είναι μια λύση τού (3.16)*, τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο $m := \prod\limits_{j=1}^{k} m_j$. *Ως εκ τούτου, το σύνολο των λύσεων τού συστήματος* (3.16) *είναι η κλάση υπολοίπων*[7]

$$x_0 + m\mathbb{Z}\ \ (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

[7]Εν προκειμένω, μπορούμε να *ταυτίζουμε* την $x_0 + m\mathbb{Z}\ \ \in \mathbb{Z}/\,(m\mathbb{Z})$ με την κλάση ισοτιμίας $[x_0]_m \in \mathbb{Z}_m$ μέσω τού ισομορφισμού (3.7).

ΑΠΟΔΕΙΞΗ. Εάν για κάθε φυσικό αριθμό n και κάθε πρώτο αριθμό p ορίσουμε ως

$$\boldsymbol{\nu}_p\,(n) := \left\{ \begin{array}{l} \text{τον εκθέτη τής μεγίστης δυνατής} \\ \text{δυνάμεως τού } p \text{ που διαιρεί τον } n \end{array} \right\} \in \mathbb{N}_0,$$

τότε, σύμφωνα με το πόρισμα 3.4.9,

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \prod_{p\ \text{πρώτος},\ p|m_1} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_1)}\mathbb{Z}) \times \cdots \times \prod_{p\ \text{πρώτος},\ p|m_k} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_k)}\mathbb{Z}),$$

και επειδή

$$m_j = \prod_{p\ \text{πρώτος},\ p|m_j} p^{\boldsymbol{\nu}_p(m_j)},\ \ \forall j \in \{1, \ldots, k\},$$

συμπεραίνουμε ότι

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}).$$

Εάν, μάλιστα, λάβει κανείς υπ' όψιν το 3.4.9 και τον (3.15), ο *τύπος ορισμού* αυτού τού ισομορφισμού είναι γνωστός, ήτοι ο

$$\mathbb{Z}/\,(m\mathbb{Z}) \ni \lambda + m\mathbb{Z} \longmapsto (\lambda + m_1\mathbb{Z}, \ldots, \lambda + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}). \quad (3.17)$$

Ιδιαιτέρως, το $(b_1 + m_1\mathbb{Z}, \ldots, b_k + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})$ διαθέτει ένα *μονοσημάντως ορισμένο αρχέτυπο*

$$x_0 + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$$

(κατά μόδιο m, όπου $x_0 \in \mathbb{Z}$), μέσω τού (3.17), οπότε έχουμε

$$x_0 + m_j\mathbb{Z} = b_j + m_j\mathbb{Z},\ \forall j \in \{1, ..., k\},$$

ήτοι k ισότητες που ισοδυναμούν με τη λύση τού συστήματος ισοτιμιών (3.16) κατά μόδιο m. □

3.4.11 Σημείωση. Για την εύρεση μιας λύσεως x_0 τού συστήματος (3.16) αρκεί, για κάθε δείκτη $j \in \{1, ..., k\}$, να προσδιορισθούν

$$u_j \in \langle m_j \rangle\,,\ \ v_j \in \langle m'_j \rangle = \bigcap_{1\le l\le k,\ l\neq j} \langle m_l \rangle\,,$$

όπου

$$m'_j := \prod_{1\le l\le k,\ l\neq j} m_l,$$

τέτοια ώστε $u_j + v_j = 1$, ή -ισοδυνάμως- $(y_j, z_j) \in \mathbb{Z}^2$, τέτοια ώστε

$$m_j y_j + m'_j z_j = 1,\ \forall j \in \{1, ..., k\}.$$

Επειδή όμως δεν θα χρειασθούμε ουσιαστικώς τα y_j, αρκεί να προσδιορίσουμε τη *μοναδική* κατά μόδιο m_j *λύση* $z_j \in \mathbb{Z}$ τής ισοτιμίας

$$m'_j z_j \equiv 1 (\mathrm{mod}\ m_j)$$

βάσει των όσων προαναφέραμε στη σημείωση 3.4.3. Εάν, επί παραδείγματι, εργασθούμε με το θεώρημα τού Euler, τότε μπορούμε να θέσουμε $z_j := m_j'^{\phi(m_j)-1}$. Από τα δεδομένα μας (βλ. (3.14), (3.15) και (3.17)) έπεται ότι το

$$\boxed{x_0 = \sum_{j=1}^{k} \frac{b_j z_j m}{m_j} = \sum_{j=1}^{k} b_j m'_j z_j = \sum_{j=1}^{k} b_j m_j'^{\phi(m_j)}} \tag{3.18}$$

-ανηγμένο κατά μόδιο m- είναι μια λύση τού συστήματος ισοτιμιών (3.16), ενώ κάθε άλλη λύση του προκύπτει κατόπιν αθροίσεως (σε αυτό) ενός ακεραίου πολλαπλασίου τού m.

3.4.12 Παράδειγμα. Το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών

$$\left.\begin{array}{l} x \equiv 1 (\mathrm{mod}\ 3) \\ x \equiv 2 (\mathrm{mod}\ 4) \\ x \equiv 3 (\mathrm{mod}\ 5) \end{array}\right\}$$

είναι η κλάση υπολοίπων $58 + 60\mathbb{Z}$ $(\in \mathbb{Z}/60\mathbb{Z})$, διότι (κατά τον τύπο (3.18))

$$\begin{aligned} x_0 &= 1 \cdot 20^{\phi(3)} + 2 \cdot 15^{\phi(4)} + 3 \cdot 12^{\phi(5)} = 1 \cdot 20^2 + 2 \cdot 15^2 + 3 \cdot 12^4 \\ &= 1 \cdot 400 + 2 \cdot 225 + 3 \cdot 20\,736 = 63\,058 \equiv 58 (\mathrm{mod}\ 60). \end{aligned}$$

Τα δύο θεωρήματα 3.4.15 και 3.4.16 που ακολουθούν αποτελούν απλές γενικεύσεις τού 3.4.10. Μέσω αυτών το πρόβλημα τής επιλύσεως γραμμικών ισοτιμιών (με έναν άγνωστο) αντιμετωπίζεται σε *πλήρη γενικότητα*.

3.4.13 Λήμμα. *Εάν $m_1, m_2 \in \mathbb{N}$ και $b_1, b_2 \in \mathbb{Z}$, τότε υπάρχει ακέραιος αριθμός x με $x \equiv b_1 (\mathrm{mod}\ m_1)$ και $x \equiv b_2 (\mathrm{mod}\ m_2)$ εάν και μόνον εάν* μκδ $(m_1, m_2) \mid b_2 - b_1$.

Απόδειξη. Εάν $x \in \mathbb{Z}$ με $x \equiv b_1 \pmod{m_1}$ και $x \equiv b_2 \pmod{m_2}$, τότε

$$\left.\begin{array}{l} m_1 \mid x - b_1 \\ m_2 \mid x - b_2 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} \text{μκδ}\,(m_1, m_2) \mid x - b_1 \\ \text{μκδ}\,(m_1, m_2) \mid x - b_2 \end{array}\right\} \Longrightarrow \text{μκδ}\,(m_1, m_2) \mid x - b_1 - (x - b_2)\,.$$

Και αντιστρόφως· εάν $d := \text{μκδ}(m_1, m_2)$ και $d \mid b_2 - b_1$, γράφοντας τον d ως ακέραιο γραμμικό συνδυασμό

$$d = k_1 m_1 + k_2 m_2, \quad k_1, k_2 \in \mathbb{Z},$$

και θέτοντας $\nu := \frac{k_1 (b_2 - b_1)}{d}$, λαμβάνουμε

$$m_1 \nu \equiv (d - k_2 m_2)\, \tfrac{(b_2 - b_1)}{d} \equiv b_2 - b_1 \,(\mathrm{mod}\, m_2)\,,$$

οπότε για τον ακέραιο αριθμό $x := b_1 + m_1 \nu$ ισχύουν οι ισοτιμίες $x \equiv b_1 (\mathrm{mod}\ m_1)$ και $x \equiv b_1 + (b_2 - b_1) \equiv b_2 (\mathrm{mod}\ m_2)$. □

3.4.14 Λήμμα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ έχουμε*

$$\text{μκδ}\left(\text{εκπ}\left(m_1, \ldots, m_{k-1}\right), m_k\right) = \text{εκπ}\left(\text{μκδ}\left(m_1, m_k\right), \ldots, \text{μκδ}\left(m_{k-1}, m_k\right)\right)$$

3.4.15 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} x \equiv b_1 (\text{mod } m_1) \\ \vdots \\ x \equiv b_k (\text{mod } m_k) \end{array} \right\} \tag{3.19}$$

είναι επιλύσιμο εάν και μόνον εάν

$$\text{μκδ}\left(m_j, m_l\right) \mid b_j - b_l, \ \forall (j,l) \in \mathbb{N}^2, \ 1 \leq j, l \leq k, \ j \neq l. \tag{3.20}$$

Μάλιστα, εάν το x_0 είναι μια λύση τού (3.19)*, τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο

$$m := \text{εκπ}\left(m_1, m_2, ..., m_k\right).$$

Ως εκ τούτου, όταν ικανοποιούνται οι συνθήκες (3.20)*, το σύνολο των λύσεων τού συστήματος* (3.19) *είναι η κλάση υπολοίπων*

$$x_0 + m\mathbb{Z} \ \ (\in \mathbb{Z}/\left(m\mathbb{Z}\right)).$$

ΑΠΟΔΕΙΞΗ. (i) Έστω x_0 είναι μια λύση τού (3.19). Τότε για κάθε $j, l \in \{1, \ldots, k\}$ με $j \neq l$ έχουμε

$$\left.\begin{array}{c} x_0 \equiv b_j \,(\text{mod } m_j) \\ x_0 \equiv b_l \,(\text{mod } m_l) \end{array}\right\} \Longrightarrow \left.\begin{array}{c} m_j \mid x_0 - b_j \\ m_l \mid x_0 - b_l \end{array}\right\} \Longrightarrow \left.\begin{array}{c} \text{μκδ}\left(m_j, m_l\right) \mid x_0 - b_j \\ \text{μκδ}\left(m_j, m_l\right) \mid x_0 - b_l \end{array}\right\} \Longrightarrow \text{(3.20)}.$$

Και αντιστρόφως· ας υποθέσουμε την ισχύ των συνθηκών (3.20).

Εργαζόμενοι επαγωγικώς θα κατασκευάσουμε για κάθε $j \in \{1, \ldots, k\}$ έναν ακέραιο αριθμό y_j, ούτως ώστε να ισχύουν οι ισοτιμίες

$$\left\{ \begin{array}{c} y_j \equiv b_1 (\text{mod } m_1) \\ \vdots \\ y_j \equiv b_j (\text{mod } m_j) \end{array} \right\}.$$

Κατ' αρχάς ορίζουμε ως y_1 έναν εκπρόσωπο τής κλάσεως υπολοίπων $[b_1]_{m_1}$. Εάν $j \in \{1, \ldots, k-1\}$ και υποθέσουμε ότι οι ακέραιοι $y_1, \ldots, y_j$ έχουν ήδη ορισθεί, κατασκευάζουμε κατάλληλο ακέραιο y_{j+1} ως ακολούθως: Επειδή

$$y_j \equiv b_l \,(\text{mod } m_l), \quad \forall l \in \{1, \ldots, j\},$$

έχουμε

$$[m_l \mid y_j - b_l,\ \forall l \in \{1, \dots, j\}] \Longrightarrow [\mu\kappa\delta\,(m_l, m_{j+1}) \mid y_j - b_l,\ \forall l \in \{1, \dots, j\}]\,.$$

Εξ υποθέσεως,

$$\mu\kappa\delta\,(m_l, m_{j+1}) \mid b_l - b_{j+1},\ \forall l \in \{1, \dots, j\}.$$

Άρα

$$\mu\kappa\delta\,(m_l, m_{j+1}) \mid (y_j - b_l) + (b_l - b_{j+1}) = y_j - b_{j+1},\ \forall l \in \{1, \dots, j\}$$

και, ως εκ τούτου,

$$\epsilon\kappa\pi\,(\mu\kappa\delta\,(m_1, m_{j+1}), \dots, \mu\kappa\delta\,(m_j, m_{j+1})) \mid y_j - b_{j+1}.$$

Εφαρμόζοντας λοιπόν το λήμμα 3.4.14 συμπεραίνουμε ότι

$$\mu\kappa\delta\,(\epsilon\kappa\pi\,(m_1, \dots, m_j), m_{j+1}) \mid y_j - b_{j+1}.$$

Κατά συνέπειαν, βάσει τού λήμματος 3.4.13 υπάρχει ένας $y_{j+1} \in \mathbb{Z}$, τέτοιος ώστε

$$y_{j+1} \equiv y_j \pmod{\epsilon\kappa\pi\,(m_1, \dots, m_j)} \qquad y_{j+1} \equiv b_{j+1} \pmod{m_{j+1}},$$

οπότε

$$[m_l \mid \epsilon\kappa\pi\,(m_1, .., m_j),\ \forall l \in \{1, .., j\}] \Longrightarrow y_{j+1} \equiv y_j \equiv b_l \pmod{m_l}, \forall l \in \{1, .., j\}.$$

(ii) Έστω τώρα $m := \epsilon\kappa\pi(m_1, m_2, ..., m_k)$ και έστω x_0 ο (μοναδικός) εκπρόσωπος τής κλάσεως υπολοίπων $[y_k]_m$ με $0 \leq x_0 < m$. Εάν ο x είναι ένας ακέραιος αριθμός, ο οποίος πληροί τις k ισοτιμίες (3.19), τότε έχουμε

$$[x \equiv b_\ell \equiv x_0 \pmod{m_\ell}, \forall \ell \in \{1, \dots, k\}]\,,$$

οπότε

$$[m_\ell \mid x_0 - x,\ \forall \ell \in \{1, \dots, k\}] \Longrightarrow m \mid x_0 - x \Longrightarrow x_0 - x \in m\mathbb{Z}.$$

Και αντιστρόφως· εάν $x \in \mathbb{Z}$ και $x \equiv x_0 \pmod{m}$, τότε έχουμε προφανώς για κάθε $\ell \in \{1, \dots, k\}$: $x \equiv b_\ell \equiv x_0 \pmod{m_\ell}$. □

3.4.16 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \dots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \dots, a_k,\ b_1, \dots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{array} \right\} \tag{3.21}$$

δεν είναι επιλύσιμο εάν δεν ικανοποιούνται ταυτοχρόνως οι συνθήκες

$$\text{μκδ}\,(a_j, m_j) \mid b_j, \quad \forall j \in \{1, ..., k\}. \tag{3.22}$$

Από την άλλη μεριά, όταν οι συνθήκες (3.22) *ικανοποιούνται, το σύνολο των λύσεων τού συστήματος* (3.21) *ταυτίζεται με το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} x \equiv c_1 \,(\mathrm{mod}\ m_1^\star) \\ \vdots \\ x \equiv c_k \,(\mathrm{mod}\ m_k^\star) \end{array} \right\} \tag{3.23}$$

όπου

$$c_j := \left(a_j^\star\right)^{\phi\left(m_j^\star\right)-1}\ b_j^\star$$

και

$$a_j^\star := \frac{a_j}{\text{μκδ}\,(a_j, m_j)},\ \ b_j^\star := \frac{b_j}{\text{μκδ}\,(a_j, m_j)},\ \ m_j^\star := \frac{m_j}{\text{μκδ}\,(a_j, m_j)},$$

για κάθε $j \in \{1, ..., k\}$ *και* ϕ *η συνάρτηση τού Euler.*

ΑΠΟΔΕΙΞΗ. Για να υπάρχουν κοινές λύσεις τού συστήματος (3.21) θα πρέπει τουλάχιστον καθεμιά των ισοτιμιών του να είναι αφ' εαυτής επιλύσιμη. Τούτο σημαίνει (επί τη βάσει τής προτάσεως 3.4.1) ότι μκδ$(a_j, m_j) \mid b_j$ για κάθε δείκτη $j \in \{1, ..., k\}$. Από την άλλη μεριά, εάν οι συνθήκες (3.22) ικανοποιούνται, εφαρμόζουμε το πόρισμα 3.4.5 για κάθε μία εκ των αρχικών ισοτιμιών και συμπεραίνουμε ότι το (3.21) ισοδυναμεί με το σύστημα

$$\left\{ \begin{array}{c} a_1^\star x \equiv b_1^\star \,(\mathrm{mod}\ m_1^\star) \\ \vdots \\ a_k^\star x \equiv b_k^\star \,(\mathrm{mod}\ m_k^\star) \end{array} \right\} \tag{3.24}$$

Επειδή μκδ$(a_j^\star, m_j^\star) = 1$, η γραμμική ισοτιμία $a_j^\star x \equiv b_j^\star \left(\mathrm{mod}\ m_j^\star\right)$ διαθέτει μοναδική λύση κατά μόδιο $m_j^\star$, ήτοι την $x \equiv c_j (\mathrm{mod}\ m_j^\star)$ (βλ. 3.4.3), οπότε το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών (3.24) ταυτίζεται με το σύνολο των λύσεων τού συστήματος (3.23). □

3.4.17 Παρατήρηση. Προφανώς, το πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.21) ανάγεται στο πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.23), ήτοι ενός συστήματος τού τύπου (3.19), οπότε αντιμετωπίζεται βάσει των όσων ελέχθησαν στο θεώρημα 3.4.15.

3.4.18 Παράδειγμα. Ας θεωρήσουμε το ακόλουθο σύστημα τριών γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{l} 2x \equiv 4 \,(\mathrm{mod}\ 8) \\ 6x \equiv 12 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\}.$$

Επειδή μκδ$(2, 8) = 2 \mid 4$, μκδ$(6, 9) = 3 \mid 12$ και μκδ$(1, 12) = 1 \mid 14$, αυτό είναι ισοδύναμο με το

$$\left\{ \begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 4) \\ 2x \equiv 4 \,(\mathrm{mod}\ 3) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\}.$$

Η δεύτερη ισοτιμία έχει ως λύση της την κλάση υπολοίπων $2 + 3\mathbb{Z}$ $(\in \mathbb{Z}/3\mathbb{Z})$, διότι $2^{\phi(3)-1} \cdot 4 = 8 \equiv 2 \,(\mathrm{mod}\ 3)$. Ως εκ τούτου, βάσει τού θεωρήματος 3.4.16 το ανωτέρω σύστημα είναι ισοδύναμο με το

$$\left\{ \begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 4) \\ x \equiv 2 \,(\mathrm{mod}\ 3) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\},$$

το οποίο διαθέτει μοναδική λύση κατά μόδιο εκπ$(4, 3, 12) = 12$, αφού

$$\text{μκδ}\,(4, 3) = 1 \mid 4 - 3, \ \ \text{μκδ}\,(12, 3) = 3 \mid 14 - 2, \ \ \text{μκδ}\,(12, 4) = 4 \mid 14 - 2$$

(βλ. θεώρημα 3.4.15). Επειδή έχουμε μκδ$(4, 3) = 1$, η μοναδική λύση x_0 (κατά μόδιο $4 \cdot 3 = 12$) των δύο πρώτων ισοτιμιών προσδιορίζεται μέσω τού θεωρήματος 3.4.10. Πράγματι· κατά τον τύπο (3.18),

$$x_0 = 2 \cdot 3^{\phi(4)} + 2 \cdot 4^{\phi(3)} = 50 \equiv 2 \,(\mathrm{mod}\ 12)\,,$$

λύση, η οποία επαληθεύει (κατ' ανάγκην!) *και* την τρίτη εκ των ανωτέρω ισοτιμιών (βλ. θεώρημα 3.4.15).

3.5 ΣΩΜΑ ΚΛΑΣΜΑΤΩΝ ΑΚΕΡΑΙΑΣ ΠΕΡΙΟΧΗΣ

Τα σώματα, από τον ίδιο τους τον ορισμό, χαίρουν λίαν ευάρεστων ιδιοτήτων, όπως, επί παραδείγματι, είναι η ύπαρξη αντιστρόφου για κάθε μη μηδενικό στοιχείο τους. Αντικείμενο τής παρούσας ενότητας είναι η απόδειξη τού ότι *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί *κατά τρόπο φυσικό* σε ένα σώμα. Αυτή επιτυγχάνεται μέσω τής γενικεύσεως τής γνωστής μεθόδου κατασκευής των ρητών αριθμών από τους ακεραίους.

3.5.1 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Επί τού $R \times (R\smallsetminus\{0_R\})$ ορίζουμε μια διμελή σχέση "$\sim$" ως ακολούθως:

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

3.5.2 Πρόταση. *Η "$\sim$" αποτελεί μια σχέση ισοδυναμίας.*

ΑΠΟΔΕΙΞΗ. Η "$\sim$" είναι *ανακλαστική*, διότι

$$ab = ba \Rightarrow (a,b) \sim (a,b)\,, \;\; \forall (a,b) \in R \times (R\smallsetminus\{0_R\})\,,$$

συμμετρική, διότι για οιαδήποτε ζεύγη $(a,b),(c,d) \in R \times (R\smallsetminus\{0_R\})$ έχουμε

$$(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)\,,$$

και, τέλος, *μεταβατική*, αφού για οιαδήποτε $(a,b),(a',b'),(a'',b'') \in R\times(R\smallsetminus\{0_R\})$ με

$$(a,b) \sim (a',b') \;\text{ και }\; (a',b') \sim (a'',b'')$$

έχουμε $ab' = ba'$ και $a'b'' = b'a''$, οπότε

$$ab''b' = ab'b'' = ba'b'' = bb'a'' = ba''b',$$

και, ως εκ τούτου,

$$\left.\begin{array}{r}(ab'' - ba'')b' = 0_R \\ b' \neq 0_R\end{array}\right\} \Longrightarrow ab'' = ba'' \Longrightarrow (a,b) \sim (a'',b'')$$

(με την πρώτη εκ των ανωτέρω συνεπαγωγών οφειλόμενη στο ότι ο δακτύλιος R είναι ακεραία περιοχή). □

3.5.3 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Ως

$$\boxed{\mathbf{Fr}(R) := (R \times (R\smallsetminus\{0_R\}))\,/\sim}$$

συμβολίζουμε το σύνολο κλάσεων ισοδυναμίας ως προς την "$\sim$". Το **κλάσμα** ενός $a \in R$ «διηρημένου» διά ενός $b \in R\smallsetminus\{0_R\}$ είναι η κλάση ισοδυναμίας

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

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

$$\begin{cases} \dfrac{a}{b} + \dfrac{c}{d} & := & \dfrac{ad+cb}{bd}, \\[2ex] \dfrac{a}{b} \cdot \dfrac{c}{d} & := & \dfrac{ac}{bd}. \end{cases}$$

3.5.4 Πρόταση. *Οι εν λόγω πράξεις είναι καλώς ορισμένες.*

ΑΠΟΔΕΙΞΗ. Εάν για κάποια ζεύγη $(a,b),(a',b')$ και $(c,d),(c',d')\in R\times(R\smallsetminus\{0_R\})$ έχουμε $[(a,b)]=[(a',b')]$ και $[(c,d)]=[(c',d')]$, τότε

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}\ \text{ και }\ \frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}.$$

Πράγματι· επειδή εξ υποθέσεως

$$\left.\begin{matrix}(a,b)\sim(a',b')\\(c,d)\sim(c',d')\end{matrix}\right\}\Longrightarrow\left.\begin{matrix}ab'=ba'\\cd'=dc'\end{matrix}\right\}\Longrightarrow\left.\begin{matrix}ab'dd'=ba'dd'\\cd'bb'=dc'bb'\end{matrix}\right\},$$

(κατόπιν προσθέσεως κατά μέλη) έπεται ότι

$$ab'dd'+cd'bb'=ba'dd'+dc'bb'\Longrightarrow(ad+cb)\,b'd'=(a'd'+c'b')\,bd,$$

ήτοι ότι

$$\tfrac{ad+cb}{bd}=\tfrac{a'd'+c'b'}{b'd'}\Longrightarrow\tfrac{a}{b}+\tfrac{c}{d}=\tfrac{a'}{b'}+\tfrac{c'}{d'}.$$

Εξάλλου, πολλαπλασιασμός κατά μέλη μάς οδηγεί στην ισότητα $ab'cd'=ba'dc'$, απ' όπου λαμβάνουμε

$$(ac)\,(b'd')=(bd)\,(a'c')\Longrightarrow\tfrac{ac}{bd}=\tfrac{a'c'}{b'd'},$$

ήτοι $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$. □

3.5.5 Θεώρημα. *Το σύνολο* $\mathbf{Fr}(R)$ *των κλασμάτων μιας ακεραίας περιοχής* R *αποτελεί ένα σώμα ως προς τις ως άνω ορισθείσες πράξεις προσθέσεως και πολλαπλασιασμού.* (*Γι' αυτόν τον λόγο το* $\mathbf{Fr}(R)$ *ονομάζεται* ***σώμα κλασμάτων*** *της ακεραίας περιοχής* R.)

ΑΠΟΔΕΙΞΗ. (i) Η "+" είναι *προσεταιριστική και μεταθετική*, διότι

$$\begin{aligned}\left(\tfrac{a}{b}+\tfrac{c}{d}\right)+\tfrac{e}{f}&=\tfrac{ad+cb}{bd}+\tfrac{e}{f}=\tfrac{adf+cbf+ebd}{bdf}\\&=\tfrac{adf+(cf+ed)b}{bdf}=\tfrac{a}{b}+\tfrac{cf+ed}{df}=\tfrac{a}{b}+\left(\tfrac{c}{d}+\tfrac{e}{f}\right)\end{aligned}$$

και $\frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd}=\frac{cb+ad}{bd}=\frac{c}{d}+\frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in\mathbf{Fr}(R)$.
(ii) Το *μηδενικό στοιχείο* (= ουδέτερο στοιχείο ως προς την "+") τού $\mathbf{Fr}(R)$ είναι το[8] $0_{\mathbf{Fr}(R)}:=\frac{0_R}{1_R}$, διότι για κάθε κλάσμα $\frac{a}{b}\in\mathbf{Fr}(R)$ έχουμε

$$\tfrac{a}{b}+\tfrac{0_R}{1_R}=\tfrac{(a\cdot1_R)+(b\cdot0_R)}{b\cdot1_R}=\tfrac{a}{b}=\tfrac{(b_R\cdot b)+(1_R\cdot a)}{1_R\cdot b}=\tfrac{0_R}{1_R}+\tfrac{a}{b}.$$

[8] Σημειωτέον ότι *για κάθε* $b\in R\smallsetminus\{0_R\}$ έχουμε $\frac{0_R}{b}=\frac{0_R}{1_R}$.

(iii) Κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ έχει το κλάσμα $\frac{-a}{b}$ ως *αντίθετό του* ως προς την "+", καθότι

$$\tfrac{a}{b} + \tfrac{-a}{b} = \tfrac{ab+(-a)b}{b^2} = \tfrac{(a+(-a))b}{b^2} = \tfrac{a+(-a)}{b} = \tfrac{0_R}{b} = \tfrac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}$$

και

$$\tfrac{-a}{b} + \tfrac{a}{b} = \tfrac{(-a)b+ab}{b^2} = \tfrac{((-a)+a)b}{b^2} = \tfrac{(-a)+a}{b} = \tfrac{0_R}{b} = \tfrac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}.$$

(iv) Η "$\cdot$" είναι *προσεταιριστική και μεταθετική*, διότι

$$\left(\tfrac{a}{b} \cdot \tfrac{c}{d}\right) \cdot \tfrac{e}{f} = \left(\tfrac{ac}{bd}\right) \cdot \tfrac{e}{f} = \tfrac{(ac)e}{(bd)f} = \tfrac{a(ce)}{b(df)} = \tfrac{a}{b} \cdot \left(\tfrac{ce}{df}\right) = \tfrac{a}{b} \cdot \left(\tfrac{c}{d} \cdot \tfrac{e}{f}\right)$$

και $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$.
(v) Η "$\cdot$" είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "+". Επειδή η "$\cdot$" είναι μεταθετική, αρκεί προς τούτο να ελεγχθεί η επιμεριστικότητα μόνον εκ δεξιών. Για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned}\left(\tfrac{a}{b} + \tfrac{c}{d}\right) \cdot \tfrac{e}{f} &= \left(\tfrac{ad+cb}{bd}\right) \cdot \tfrac{e}{f} = \tfrac{(ad+cb)e}{(bd)f} = \tfrac{ade+cbe}{bdf} = \tfrac{ade}{bdf} + \tfrac{cbe}{bdf} \\ &= \tfrac{ae}{bf} + \tfrac{ce}{df} = \left(\tfrac{a}{b} \cdot \tfrac{e}{f}\right) + \left(\tfrac{c}{d} \cdot \tfrac{e}{f}\right).\end{aligned}$$

(vi) Το $1_{\mathbf{Fr}(R)} := \frac{1_R}{1_R}$ είναι *μοναδιαίο στοιχείο*[9] (= ουδέτερο στοιχείο ως προς την "$\cdot$") τού $\mathbf{Fr}(R)$, διότι για κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ ισχύουν οι ισότητες

$$\tfrac{a}{b} \cdot 1_{\mathbf{Fr}(R)} = \tfrac{a}{b} \cdot \tfrac{1_R}{1_R} = \tfrac{a \cdot 1_R}{b \cdot 1_R} = \tfrac{a}{b} = \tfrac{1_R \cdot a}{1_R \cdot b} = \tfrac{1_R}{1_R} \cdot \tfrac{a}{b} = 1_{\mathbf{Fr}(R)} \cdot \tfrac{a}{b}.$$

(vii) Εκ των (i)-(vi) συνάγεται ότι η τριάδα $(\mathbf{Fr}(R), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Επομένως, για να αποδείξουμε, επιπροσθέτως, ότι αυτός ο δακτύλιος είναι και *σώμα*, αρκεί να αποδείξουμε ότι οιοδήποτε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R) \setminus \{0_{\mathbf{Fr}(R)}\}$ είναι αντιστρέψιμο. Επειδή από τη συνθήκη $\frac{a}{b} \neq \frac{0_R}{1_R}$ προκύπτει ότι

$$a = a \cdot 1_R \neq 0_R \cdot b = 0_R \Longrightarrow \tfrac{b}{a} \in \mathbf{Fr}(R),$$

εκ των ισοτήτων

$$\tfrac{a}{b} \cdot \tfrac{b}{a} = \tfrac{ab}{ba} = \tfrac{ab}{ab} = \tfrac{1_R}{1_R} = 1_{\mathbf{Fr}(R)} = \tfrac{ba}{ba} = \tfrac{ba}{ab} = \tfrac{b}{a} \cdot \tfrac{a}{b}$$

συμπεραίνουμε ότι το $\frac{b}{a}$ είναι *το αντίστροφο* τού $\frac{a}{b}$. □

3.5.6 Παραδείγματα. (i) Προφανώς, $\mathbf{Fr}(\mathbb{Z}) = \mathbb{Q}$.
(ii) Εάν το K είναι ένα σώμα, το

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

[9] Σημειωτέον ότι *για κάθε* $c \in R \setminus \{0_R\}$ έχουμε $\frac{c}{c} = 1_{\mathbf{Fr}(R)}$.

καλείται **σώμα των ρητών συναρτήσεων** ή **των ρητών εκφράσεων μιας απροσδιορίστου** X **υπεράνω τού** K. Κατ' αναλογίαν, το

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

είναι το **σώμα των ρητών συναρτήσεων** n **απροσδιορίστων** $\mathsf{X}_1,..,\mathsf{X}_n$ **υπεράνω τού** K.

(iii) Εντός τής ακεραίας περιοχής $\mathbb{C}[\![\mathsf{Z}]\!]$ των επίτυπων δυναμοσειρών μιας μιγαδικής απροσδιορίστου Z (ήτοι μιας απροσδιορίστου Z υπεράνω τού $\mathbb{C}$) ορίζεται η υποπεριοχή

$$\mathbb{C}\{\mathsf{Z}\} := \left\{ \sum_{i=0}^{\infty} a_i \mathsf{Z}^i \in \mathbb{C}[\![\mathsf{Z}]\!] \,\middle|\, \sum_{i=0}^{\infty} a_i z^i \text{ συγκλίνουσα για κάθε } z \in \mathbb{C} \right\}.$$

Ως γνωστόν[10], $\mathbb{C}\{\mathsf{Z}\} = \mathcal{O}(\mathbb{C})$, όπου

$$\boxed{\mathcal{O}(\mathbb{C}) := \{\text{συναρτήσεις } f : \mathbb{C} \longrightarrow \mathbb{C} \,|\, f \text{ ολόμορφη}\}}$$

η ακεραία περιοχή των λεγομένων **ακεραίων συναρτήσεων** μιας μιγαδικής μεταβλητής. Το σώμα κλασμάτων της

$$\boxed{\mathcal{M}(\mathbb{C}) := \mathbf{Fr}(\mathcal{O}(\mathbb{C}))}$$

καλείται **σώμα των μερομόρφων συναρτήσεων** επί τού $\mathbb{C}$ (και τα στοιχεία του **μερόμορφες συναρτήσεις** επί τού $\mathbb{C}$, τις οποίες συναντούμε συχνά στο μάθημα τής Μιγαδικής Αναλύσεως).

(iv) Έστω R μια ακεραία περιοχή. Τότε

$$\boxed{\mathbf{Fr}(R[\mathsf{X}]) = \mathbf{Fr}(R)(\mathsf{X}) \ (:= \mathbf{Fr}(\mathbf{Fr}(R)[\mathsf{X}])),}$$

διότι έχουμε αφ' ενός μεν

$$\mathbf{Fr}(R[\mathsf{X}]) = \left\{ \frac{a_0 + a_1\mathsf{X} + \cdots + a_n\mathsf{X}^n}{b_0 + b_1\mathsf{X} + \cdots + b_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m,n \in \mathbb{N}_0, a_0,\dots,a_n,b_0,\dots,b_m \in R \\ \text{με } b_j \neq 0_R \text{ για κάποιον } j \in \{0,\dots,m\} \end{array} \right\},$$

αφ' ετέρου δε

$$\begin{aligned} \mathbf{Fr}(R)(\mathsf{X}) &= \left\{ \tfrac{r_0 + r_1\mathsf{X} + \cdots + r_n\mathsf{X}^n}{s_0 + s_1\mathsf{X} + \cdots + s_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m,n \in \mathbb{N}_0, r_0,\dots,r_n,s_0,\dots,s_m \in \mathbf{Fr}(R) \\ \text{με } s_j \neq 0_{\mathbf{Fr}(R)} \text{ για κάποιον } j \in \{0,\dots,m\} \end{array} \right\} \\ &= \left\{ \frac{\frac{a_0}{b_0} + \left(\frac{a_1}{b_1}\right)\mathsf{X} + \cdots + \left(\frac{a_n}{b_n}\right)\mathsf{X}^n}{\frac{c_0}{d_0} + \left(\frac{c_1}{d_1}\right)\mathsf{X} + \cdots + \left(\frac{c_m}{d_m}\right)\mathsf{X}^m} \,\middle|\, \begin{array}{c} r_i = \frac{a_i}{b_i},\ s_j = \frac{c_j}{d_j}, \\ \text{όπου } (a_i,b_i),(c_j,d_j) \in R \times (R \smallsetminus \{0_R\}), \\ \forall (i,j) \in \{0,\dots,n\} \times \{0,\dots,m\} \end{array} \right\} \\ &= \mathbf{Fr}(R[\mathsf{X}]), \end{aligned}$$

[10] Κάθε *ολόμορφη συνάρτηση* $f : \mathbb{C} \longrightarrow \mathbb{C}$ (ήτοι κάθε συνάρτηση $f : \mathbb{C} \longrightarrow \mathbb{C}$ διαθέτουσα μιγαδική παράγωγο σε κάθε σημείο τού $\mathbb{C}$) είναι *παραστάσιμη ως συγκλίνουσα δυναμοσειρά*.

με την τελευταία ισότητα προκύπτουσα ύστερα από απαλοιφή παρονομαστών.

(v) Εάν το K είναι ένα σώμα, τότε το σώμα των κλασμάτων τής ακεραίας περιοχής $K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας απροσδιορίστου X με συντελεστές ειλημμένους από το K συμβολίζεται συντόμως ως ακολούθως:

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

Σημειωτέον ότι

$$\boxed{K(\!(\mathsf{X})\!) = \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]}$$

(βλ. άσκηση **1-52**). Πράγματι· για τυχόν στοιχείο

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} \in K(\!(\mathsf{X})\!)$$

παρατηρούμε τα εξής: Εάν $b_0 \neq 0_K$, τότε $\sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]^\times$ (βλ. 1.3.9 (iii)) και

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} = \left(\sum_{i=0}^{\infty} a_i \mathsf{X}^i\right)\left(\sum_{i=0}^{\infty} b_i \mathsf{X}^i\right)^{-1} \in K[\![\mathsf{X}]\!].$$

Εάν $b_0 = 0_K$, τότε $l := \mathrm{ord}(\sum_{i=0}^{\infty} b_i \mathsf{X}^i) \geq 1$ (βλ. 1.3.4), οπότε

$$b_0 = \cdots = b_{l-1} = 0_K,\ b_l \neq 0_K \Rightarrow \sum_{i=l}^{\infty} b_i \mathsf{X}^{i-l} \in K[\![\mathsf{X}]\!]^\times$$

και

$$\frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=0}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\mathsf{X}^l \left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i \left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)^{-1}}{\mathsf{X}^l}.$$

Κατά συνέπειαν,

$$\begin{aligned} K(\!(\mathsf{X})\!) &= \left\{ \frac{\sum_{i=0}^{\infty} c_i \mathsf{X}^i}{\mathsf{X}^l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \left\{ \sum_{i=0}^{l-1} c_i \mathsf{X}^{i-l} + \sum_{i=l}^{\infty} c_i \mathsf{X}^{i-l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]. \end{aligned}$$

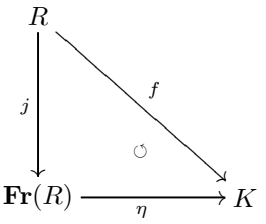
3.5.7 Πρόταση. *Κάθε ακεραία περιοχή εμφυτεύεται στο σώμα των κλασμάτων της.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα ακεραία περιοχή. Τότε ο ομομορφισμός

$$j : R \longrightarrow \mathbf{Fr}(R), \quad a \longmapsto j(a) := \tfrac{a}{1_R}, \tag{3.25}$$

είναι ένας μονομορφισμός, διότι έχει το $\{\, a \in R \mid \frac{a}{1_R} = \frac{0_R}{1_R}\} = \{0_R\}$ ως πυρήνα του (βλ. πρόταση 3.1.16). □

3.5.8 Πρόταση. (“**Καθολική ιδιότητα**” **τού** $\mathbf{Fr}(R)$.) *Έστω* R *μια ακεραία περιοχή. Τότε για κάθε μονομορφισμό* $f : R \longrightarrow K$, *όπου* K *ένα σώμα, υφίσταται ένας και μόνον μονομορφισμός σωμάτων* $\eta : \mathbf{Fr}(R) \longrightarrow K$ *ο οποίος καθιστά το διάγραμμα*



μεταθετικό (*ήτοι* $f = \eta \circ j$), *όπου* j *ο μονομορφισμός* (3.25).

ΑΠΟΔΕΙΞΗ. Ορίζουμε την $\eta : \mathbf{Fr}(R) \longrightarrow K$ μέσω τού τύπου

$$\eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1}, \ \ \forall \tfrac{a}{b} \in \mathbf{Fr}(R).$$

Η η είναι *καλώς ορισμένη* απεικόνιση, διότι για $\frac{a}{b}, \frac{a'}{b'} \in \mathbf{Fr}(R)$ με $\frac{a}{b} = \frac{a'}{b'}$ έχουμε

$$ab' = ba' \Rightarrow f(a)f(b') = f(ab') = f(ba') = f(b)f(a'),$$

οπότε

$$f(b), f(b') \in \mathbf{Fr}(R)^{\times} \Rightarrow \eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1} = f(a')\, f(b')^{-1} =: \eta(\tfrac{a'}{b'}).$$

Η η είναι *ομομορφισμός*, καθότι για οιαδήποτε $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \eta(\tfrac{a}{b} + \tfrac{c}{d}) &= \eta(\tfrac{ad+cb}{bd}) = f(ad+cb)\, f(bd)^{-1} \\ &= (f(a)f(d) + f(c)f(b))\, f(b)f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)\, f(d)^{-1} = \eta(\tfrac{a}{b}) + \eta(\tfrac{c}{d}) \end{aligned}$$

και

$$\begin{aligned} \eta(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= \eta(\tfrac{ac}{bd}) = f(ac)\, f(bd)^{-1} \\ &= \left(f(a)f(b)^{-1}\right)\left(f(c)\, f(d)^{-1}\right) \\ &= \eta(\tfrac{a}{b})\eta(\tfrac{c}{d}). \end{aligned}$$

Η η είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ με $\eta(\frac{a}{b}) = \eta(\frac{c}{d})$, τότε

$$f(a)\, f(b)^{-1} = f(c)\, f(d)^{-1} \Rightarrow f(a)\, f(d) = f(b)\, f(c),$$

ήτοι

$$f(ad) = f(bc) \underset{[f \text{ ένριψη}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

απ' όπου έπεται ότι η η είναι πράγματι ένας *μονομορφισμός*. Προφανώς,

$$(\eta \circ j)(a) = \eta(j(a)) = \eta(\tfrac{a}{1_R}) = f(a)f(1_R)^{-1} = f(a) \cdot 1_K = f(a)$$

για κάθε $a \in R$, οπότε $f = \eta \circ j$. Τέλος, εάν υποτεθεί ότι υφίσταται κάποιος μονομορφισμός $\eta' : \mathbf{Fr}(R) \longrightarrow K$ για τον οποίο ισχύει η ισότητα $f = \eta' \circ j$, τότε για κάθε $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \eta'(\tfrac{a}{b}) &= \eta'(j(a)j(b^{-1})) = \eta'(j(ab^{-1})) = (\eta' \circ j)(ab^{-1}) \\ &= f(ab^{-1}) = f(a)f(b)^{-1} = \eta(\tfrac{a}{b}), \end{aligned}$$

απ' όπου έπεται ότι $\eta' = \eta$. □

3.5.9 Πόρισμα. *Εάν η R είναι μια ακεραία περιοχή περιεχόμενη σε ένα σώμα K, τότε το*

$$\overline{R} := \left\{ ab^{-1} \middle| \, (a,b) \in R \times (R \smallsetminus \{0_R\}) \right\} \subseteq K$$

είναι το ελάχιστο υπόσωμα τού K (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την R και $\overline{R} \cong \mathbf{Fr}(R)$.

ΑΠΟΔΕΙΞΗ. Έστω $\iota : R \hookrightarrow K$ η συνήθης ένθεση. Επειδή η ι είναι μονομορφισμός, η πρόταση 3.5.8 μας πληροφορεί ότι υφίσταται ένας και μόνον μονομορφισμός σωμάτων $\eta : \mathbf{Fr}(R) \longrightarrow K$ με $\iota = \eta \circ j$, όπου j ο μονομορφισμός (3.25). Για κάθε $(a,b) \in R \times (R \smallsetminus \{0_R\})$ έχουμε

$$\eta(\tfrac{a}{b}) = \eta(j(a)j(b^{-1})) = \eta(j(ab^{-1})) = (\eta \circ j)(ab^{-1}) = \iota(ab^{-1}) = ab^{-1},$$

οπότε $\overline{R} = \mathrm{Im}(\eta) \cong \mathbf{Fr}(R)$. Επομένως, το $\overline{R}$ είναι αφ' εαυτού σώμα (βλ. 3.1.11 (iii)) με $R \subseteq \overline{R}$. Έστω τώρα τυχόν υπόσωμα L τού K περιέχον την ακεραία περιοχή R. Το L περιέχει το b^{-1} για κάθε $b \in R \smallsetminus \{0_R\}$. Κατά συνέπειαν, το L περιέχει όλα τα στοιχεία τής μορφής ab^{-1}, όπου $(a,b) \in R \times (R \smallsetminus \{0_R\})$. Αυτό σημαίνει ότι $R \subseteq L \subseteq \overline{R} \cong \mathbf{Fr}(R)$. □

3.5.10 Παράδειγμα. Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ περιέχεται (εξ ορισμού) στο σώμα $\mathbb{Q}(\sqrt{2})$ (βλ. άσκηση **1-44**). Επομένως,

$$\mathbb{Z}[\sqrt{2}] \subseteq \overline{\mathbb{Z}[\sqrt{2}]} = \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \subseteq \mathbb{Q}(\sqrt{2}).$$

Από την άλλη μεριά, κάθε στοιχείο τού $\mathbb{Q}(\sqrt{2})$ είναι τής μορφής $r + s\sqrt{2}$, όπου $r, s \in \mathbb{Q}$. Γράφοντας τα r, s ως κλάσματα $r = \frac{a}{b}$, $s = \frac{c}{d}$, για κατάλληλα ζεύγη $(a,b), (c,d) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, παρατηρούμε ότι

$$r + s\sqrt{2} = \tfrac{a}{b} + \tfrac{c}{d}\sqrt{2} = \tfrac{ad+cb\sqrt{2}}{bd} \in \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]).$$

Εκ των ανωτέρω έπεται ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$.

3.5.11 Πόρισμα. *Για κάθε σώμα K υφίσταται ισομορφισμός $K \cong \mathbf{Fr}(K)$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού πορίσματος 3.5.9 στην ειδική περίπτωση κατά την οποία $R = K$ (καθόσον $\overline{K} = K$). □

3.5.12 Πρόταση. *Έστω $f : R_1 \longrightarrow R_2$ ένας ομομορφισμός ακεραίων περιοχών. Τότε η απεικόνιση*

$$\mathbf{Fr}(f) : \mathbf{Fr}(R_1) \longrightarrow \mathbf{Fr}(R_2),\ \mathbf{Fr}(f)(\tfrac{a}{b}) := \tfrac{f(a)}{f(b)},\ \forall\,(a,b) \in R_1 \times (R_1 \smallsetminus \{0_{R_1}\}),$$

η επαγομένη μέσω τού f είναι ομομορφισμός σωμάτων. Επιπροσθέτως, ισχύουν τα εξής:

(i) *Εάν ο f είναι μονομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι μονομορφισμός.*

(ii) *Εάν ο f είναι επιμορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι επιμορφισμός.*

(iii) *Εάν ο f είναι ισομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι ισομορφισμός, οπότε*

$$R_1 \cong R_2 \Longrightarrow \mathbf{Fr}(R_1) \cong \mathbf{Fr}(R_2).$$

ΑΠΟΔΕΙΞΗ. Η $\mathbf{Fr}(f)$ είναι *ομομορφισμός* σωμάτων, διότι για $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ έχουμε

$$\begin{aligned} \mathbf{Fr}(f)(\tfrac{a}{b} + \tfrac{c}{d}) &= \mathbf{Fr}(f)(\tfrac{ad+cb}{bd}) = \tfrac{f(ad+cb)}{f(bd)} = \tfrac{f(ad)+f(cb)}{f(b)f(d)} = \tfrac{f(a)f(d)+f(c)f(b)}{f(b)f(d)} \\ &= \tfrac{f(a)}{f(b)} + \tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b}) + \mathbf{Fr}(f)(\tfrac{c}{d}) \end{aligned}$$

και

$$\begin{aligned} \mathbf{Fr}(f)(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= \mathbf{Fr}(f)(\tfrac{ac}{bd}) = \tfrac{f(ac)}{f(bd)} = \tfrac{f(a)f(c)}{f(b)f(d)} \\ &= \tfrac{f(a)}{f(b)}\tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b})\mathbf{Fr}(f)(\tfrac{c}{d}). \end{aligned}$$

(i) Εάν η f είναι ενριπτική, τότε και η απεικόνιση $\mathbf{Fr}(f)$ είναι ενριπτική, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ με $\mathbf{Fr}(f)(\frac{a}{b}) = \mathbf{Fr}(\frac{c}{d})$, τότε $\frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$, απ' όπου έπεται ότι

$$f(a)f(d) = f(c)f(b) \Longrightarrow f(ad) = f(cb) \underset{[f \text{ ενριπτική}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

(ii) Εάν η f είναι επιρριπτική, τότε και η $\mathbf{Fr}(f)$ είναι επιρριπτική, διότι για κάθε $\frac{c}{d} \in \mathbf{Fr}(R_2)$ υπάρχει ζεύγος $(a,b) \in R_1 \times (R_1 \smallsetminus \{0_{R_1}\})$, τέτοιο ώστε να ισχύει

$$[f(a) = c, \quad f(b) = d] \Longrightarrow \mathbf{Fr}(f)(\tfrac{a}{b}) = \tfrac{f(a)}{f(b)},$$

ήτοι $\mathbf{Fr}(f)(\frac{a}{b}) = \frac{c}{d}$. Το (iii) είναι άμεση συνέπεια των (i) και (ii). □

3.6 ΠΡΩΤΑ ΣΩΜΑΤΑ

Έστω L ένα υπόσωμα τού σώματος $\mathbb{Q}$ των ρητών αριθμών. Επειδή υπάρχει πάντοτε κάποιο $a \in L\setminus\{0\}$, η -εξ ορισμού εγγυηθείσα- ύπαρξη τού (πολλαπλασιαστικού) αντιστρόφου του a^{-1} έχει ως επακόλουθο το ότι

$$a^{-1}a = 1_L = 1_{\mathbb{Q}} \in L.$$

Ως εκ τούτου, για κάθε ακέραιο $n \in \mathbb{Z}$ ισχύει $n = n \cdot 1_L = n \cdot 1_{\mathbb{Q}} \in L$, οπότε έχουμε κατ' ανάγκην την εγκλειστική σχέση $\mathbb{Z} \subseteq L \subseteq \mathbb{Q}$. Όμως, σύμφωνα με το πόρισμα 3.5.9, το $\mathbb{Q} = \mathbf{Fr}\,(\mathbb{Z})$ είναι το ελάχιστο σώμα (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την ακεραία περιοχή $\mathbb{Z}$. Άρα τελικώς $L = \mathbb{Q}$. Η ιδιότητα αυτή τού $\mathbb{Q}$ το καθιστά το πλέον τυπικό παράδειγμα των λεγομένων «πρώτων σωμάτων».

3.6.1 Ορισμός. Ένα σώμα K καλείται **πρώτο σώμα** όταν δεν περιέχει κανένα γνήσιο υπόσωμα.

3.6.2 Παράδειγμα. Πέραν τού $\mathbb{Q}$, ένα άλλο πρώτο σώμα είναι το $\mathbb{Z}_p$, όπου p πρώτος αριθμός. Πράγματι· εάν το L είναι ένα υπόσωμα τού $\mathbb{Z}_p$, τότε η (προσθετική) υποομάδα $(L,+)$ τής ομάδας $(\mathbb{Z}_p,+)$ είναι πεπερασμένη με τάξη της έναν διαιρέτη τού p (λόγω τού θεωρήματος τού Lagrange). Επειδή λοιπόν ο p είναι πρώτος, $|L| = 1$ ή $|L| = p$. Η πρώτη περίπτωση αποκλείεται, καθότι το L -ως σώμα- έχει τάξη $|L| \geq 2$. Επομένως, $|L| = p$, οπότε κατ' ανάγκην $L = \mathbb{Z}_p$.

3.6.3 Θεώρημα. *Κάθε σώμα K περιέχει ένα και μόνον πρώτο υπόσωμα.*

ΑΠΟΔΕΙΞΗ. Το σώμα

$$K_0 := \bigcap\{\, S \mid S \text{ υπόσωμα τού } K\} \subseteq K$$

είναι ένα πρώτο υπόσωμα τού K. Πράγματι· εάν το L είναι ένα υπόσωμα τού K_0, τότε το L είναι και υπόσωμα τού K, οπότε $K_0 \subseteq L$, απ' όπου συμπεραίνουμε ότι $L = K_0$. Υπολείπεται η απόδειξη τής μοναδικότητας τού K_0. Υποτιθεμένης τής ύπαρξεως ενός άλλου πρώτου υποσώματος K_0' τού σώματος K, το $K_0 \cap K_0'$ είναι υπόσωμα τού K και $K_0 \cap K_0' \subseteq K_0$, $K_0 \cap K_0' \subseteq K_0'$. Επομένως, $K_0 \cap K_0' = K_0$ και $K_0 \cap K_0' = K_0'$, πράγμα που σημαίνει ότι $K_0 = K_0'$. □

3.6.4 Θεώρημα. (i) *Κάθε πρώτο σώμα χαρακτηριστικής μηδέν είναι ισόμορφο με το σώμα $\mathbb{Q}$ των ρητών αριθμών.*

(ii) *Κάθε πρώτο σώμα χαρακτηριστικής p (όπου p πρώτος αριθμός) είναι ισόμορφο με το σώμα $\mathbb{Z}_p$ των κλάσεων ισοτιμιών κατά μόδιο p.*

ΑΠΟΔΕΙΞΗ. Έστω L ένα πρώτο σώμα. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow L, \quad f(n) := n \cdot 1_L, \ \ \forall n \in \mathbb{Z}.$$

Επειδή

$$\begin{cases} f(m+n) = (m+n)\cdot 1_L = m\cdot 1_L + n\cdot 1_L = f(m)+f(n), \\ f(mn) = (mn)\cdot 1_L = m\,(n\cdot 1_L) = (m\cdot 1_L)\,(n\cdot 1_L) = f(m)f(n), \end{cases}$$

για οιουσδήποτε $m, n \in \mathbb{Z}$, η f είναι ένας ομομορφισμός δακτυλίων. Βάσει τού 1ου θεωρήματος ισομορφισμών 3.3.3,

$$\mathbb{Z}/\mathbf{Ker}\,(f) \cong \mathrm{Im}\,(f) = f(\mathbb{Z}),$$

όπου

$$\mathbf{Ker}\,(f) = \{\, n \in \mathbb{Z} \mid \; n\cdot 1_L = 0_L \}.$$

(i) Εάν το L έχει χαρακτηριστική μηδέν, τότε $\mathbf{Ker}(f) = \{0\}$, οπότε

$$\mathbb{Z}/\mathbf{Ker}\,(f) = \mathbb{Z}/\{0\} \cong \mathbb{Z} \cong \mathrm{Im}\,(f) = f(\mathbb{Z}).$$

Ως εκ τούτου, η $\mathrm{Im}\,(f)$ είναι μια ακεραία περιοχή (ισόμορφη με τον $\mathbb{Z}$) και, επειδή $\mathrm{Im}\,(f) \subseteq L$, έχουμε

$$\mathbf{Fr}\,(\mathrm{Im}\,(f)) = \left\{ \frac{n\cdot 1_L}{m\cdot 1_L} \;\middle|\; (n,m) \in \mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\}) \right\} \subseteq \mathbf{Fr}\,(L) \cong L,$$

οπότε $L \cong \mathbf{Fr}\,(L) = \mathbf{Fr}\,(\mathrm{Im}\,(f)) \cong \mathbf{Fr}\,(\mathbb{Z}) = \mathbb{Q}$ (λόγω τής προτάσεως 3.5.12 και τού ότι το L είναι πρώτο σώμα).

(ii) Εάν το L έχει χαρακτηριστική p, όπου p πρώτος αριθμός, τότε, βάσει τής προτάσεως 1.4.3 έχουμε

$$p = \min\{\, |k| \in \mathbb{N} \mid \; k \in \mathbb{Z}\smallsetminus\{0\} \;\text{ με }\; k\cdot 1_L = 0_L \},$$

οπότε $p \in \mathbf{Ker}(f) \Longrightarrow p\mathbb{Z} = \langle p\rangle \subseteq \mathbf{Ker}(f)$. Αλλά και για κάθε $\lambda \in \mathbf{Ker}(f)$, γράφοντας

$$\lambda = up + r, \;\; u, r \in \mathbb{Z}, \quad 0 \le r \le p-1,$$

λαμβάνουμε

$$0_L = \lambda\cdot 1_L = u\,(p\cdot 1_L) + (r\cdot 1_L) = 0_L + r\cdot 1_L = r\cdot 1_L,$$

ήτοι μια ισότητα η οποία (λόγω τής ως άνω συνθήκης ελαχίστου που πληροί το p) ισχύει μόνον όταν $r = 0$. Επομένως, $\lambda \in \langle p\rangle$, οπότε $\mathbf{Ker}(f) \subseteq p\mathbb{Z} = \langle p\rangle$. Τελικώς λοιπόν $\mathbf{Ker}(f) = p\mathbb{Z} = \langle p\rangle$ και

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p \cong \mathrm{Im}\,(f) = f(\mathbb{Z}) = \{\, n\cdot 1_L \mid \; n \in \{0, 1, \ldots, p-1\}\} \subseteq L,$$

απ' όπου συμπεραίνουμε ότι $L = \mathrm{Im}\,(f) \cong \mathbb{Z}_p$, διότι το L είναι πρώτο σώμα. □

3.6.5 Πόρισμα. *Κάθε σώμα K περιέχει ένα υπόσωμα L, τέτοιο ώστε*:

$$L \cong \begin{cases} \mathbb{Q}, & \text{όταν } \chi\alpha\rho(K) = 0, \\ \\ \mathbb{Z}_p, & \text{όταν } \chi\alpha\rho(K) = p > 0. \end{cases}$$

3.6.6 Παρατήρηση. Σύμφωνα με όσα αναφέραμε στην απόδειξη τού θεωρήματος 3.6.4, εάν το L είναι ένα πρώτο σώμα, τότε

$$L \cong \left\{ (n \cdot 1_L)\,(m \cdot 1_L)^{-1} \;\middle|\; (n,m) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \right\}, \quad \text{όταν } \chi\alpha\rho(L) = 0,$$

και

$$L = \{ n \cdot 1_L \mid n \in \{0, 1, \ldots, p-1\} \}, \quad \text{όταν } \chi\alpha\rho(L) = p > 0.$$

Ασκήσεις

3-1. Ποιες εκ των ακολούθων απεικονίσεων $f : R \longrightarrow R'$ είναι ομομορφισμοί δακτυλίων;

(i) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k]_m .$$

(ii) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k+1]_m .$$

(iii) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a.$$

(iv) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a + d.$$

(v) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := ad - bc.$$

(vi) $R = \mathbb{Z}$, $R' = \mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := \begin{pmatrix} [1]_m & [0]_m \\ [0]_m & [k]_m \end{pmatrix}.$$

3-2. (i) Να αποδειχθεί ότι η απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5,\ n \longmapsto f(n) := ([n]_3\,, [n]_5),$$

είναι επιμορφισμός και να προσδιορισθεί ο πυρήνας $\mathrm{Ker}(f)$.

(ii) Να προσδιορισθούν όλοι οι ομομορφισμοί $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_{12}$.

3-3. Να αποδειχθεί ότι οι μόνοι ενδομορφισμοί τού $\mathbb{Z}$ είναι ο μηδενικός ομομορφισμός και ο ταυτοτικός $\mathrm{id}_{\mathbb{Z}}$.

3-4. Έστω $m \in \mathbb{N}$. Να αποδειχθεί ότι κάθε ενδομορφισμός $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ τού $\mathbb{Z}_m$ ορίζεται μέσω ενός τύπου τής μορφής

$$f([k]_m) = [a]_m\,[k]_m\,,\ \forall k \in \mathbb{Z},$$

για κάποιον ακέραιο a, τέτοιον ώστε το στοιχείο $[a]_m \in \mathbb{Z}_m$ να είναι ταυτοδύναμο.

3-5. Να αποδειχθεί ότι για κάθε ακέραιο m στερούμενον τετραγώνων η απεικόνιση

$$\mathbb{Q}(\sqrt{m}) \ni a + b\sqrt{m} \longmapsto a - b\sqrt{m} \in \mathbb{Q}(\sqrt{m}),\ \ a, b \in \mathbb{Z},$$

είναι αυτομορφισμός τού σώματος $\mathbb{Q}(\sqrt{m})$ (βλ. το (iv) τής ασκήσεως **1-44**).

3-6. Έστω K ένα σώμα με $\mathrm{χαρ}(K) = p > 0$ και έστω

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

η απεικόνιση τού Frobenius. (Βλ. 3.1.3 (iv).) Να αποδειχθούν τα εξής:

(i) Η f είναι μονομορφισμός. [*Υπόδειξη*: Βλ. πρόταση 3.1.12.]

(ii) Όταν το K είναι πεπερασμένο σώμα, τότε η f είναι ισομορφισμός (ήτοι αυτομορφισμός τού K).

(iii) Όταν το K είναι απειροπληθές, τότε η f είναι δεν είναι κατ' ανάγκην ισομορφισμός. [*Υπόδειξη*: Να εξετασθεί τι συμβαίνει στην περίπτωση κατά την οποία το K είναι το σώμα $\mathbb{Z}_p(\mathsf{X})$ των ρητών συναρτήσεων υπεράνω τού σώματος $\mathbb{Z}_p$.]

3-7. Έστω R ένας δακτύλιος και έστω $f : R \longrightarrow R$ ένας ενδομορφισμός αυτού. Να αποδειχθεί ότι το $S := \{r \in R |\ f(r) = r\}$ είναι ένας υποδακτύλιος τού R.

3-8. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν $a \in R^\times$, να αποδειχθεί ότι η απεικόνιση

$$f_a : R \longrightarrow R,\ \ r \longmapsto f_a(r) := ara^{-1},$$

είναι ένας αυτομορφισμός τού R.

3-9. Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ομομορφισμοί δακτυλίων, να αποδειχθεί ότι ισχύουν οι εγκλεισμοί:

$$\text{Ker}(f) \subseteq \text{Ker}(g \circ f), \;\; \text{Im}(g \circ f) \subseteq \text{Im}(g).$$

και ότι εξ αυτών έπονται άμεσα οι συνεπαγωγές

$$g \circ f \text{ μονομορφισμός } \Rightarrow f \text{ μονομορφισμός}$$

και

$$g \circ f \;\text{ επιμορφισμός } \Rightarrow g \text{ επιμορφισμός.}$$

Εν συνεχεία, να παρατεθούν παραδείγματα ομομορφισμών

$$f : R \longrightarrow R' \;\text{ και }\; g : R' \longrightarrow R'',$$

ούτως ώστε

(i) η σύνθεση $g \circ f$ να είναι και ο g να μην είναι μονομορφισμός,

(ii) η σύνθεση $g \circ f$ να είναι και ο f να μην είναι επιμορφισμός, και

(iii) η $g \circ f$ να είναι ισομορφισμός και κανείς εκ των f, g να μην είναι ισομορφισμός.

3-10. Έστω $f : R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων. Να αποδειχθούν τα εξής:

(i) $f(Z(R)) \subseteq Z(R')$. **(Βλ. άσκηση 1-20.)**

(ii) Εάν το $a \in R$ είναι ταυτοδύναμο στοιχείο, τότε και το $f(a) \in R'$ είναι ταυτοδύναμο.

(iii) Εάν το $a \in R$ είναι μηδενοδύναμο στοιχείο, τότε και το $f(a) \in R'$ είναι μηδενοδύναμο (οπότε $f(\text{Nil}(R)) \subseteq \text{Nil}(R')$).

Εν συνεχεία, να δοθούν παραδείγματα επιμορφισμών δακτυλίων για τους οποίους ο εγκλεισμός στο (i) είναι αυστηρός και τα αντίστροφα των (ii) και (iii) αναληθή.

3-11. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού R, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f\,(I + J) = f\,(I) + f\,(J)\,,$

(ii) $f\,(I\,J) = f\,(I)\;f\,(J)\,,$

(iii) $f\,(I \cap J) \subseteq f\,(I) \cap f\,(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$ ή $\text{Ker}(f) \subseteq J$).

(iv) Εάν ο R (και -κατ' επέκταση- και ο S, λόγω τής 3.1.5 (vii)) είναι μεταθετικός, τότε $f\,(I : J) \subseteq f\,(I) \;:\; f\,(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$).

(v) Εάν ο R είναι μεταθετικός, τότε $f(\text{Rad}(I)) \subseteq \text{Rad}(f(I))$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$).

3-12. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού S, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f^{-1}(I + J) = f^{-1}(I) + f^{-1}(J)$,

(ii) $f^{-1}(I\,J) \supseteq f^{-1}(I)\; f^{-1}(J)$, (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\mathrm{Ker}(f) \subseteq f^{-1}(I)\; f^{-1}(J)$),

(iii) $f^{-1}(I \cap J) = f^{-1}(I) \cap f^{-1}(J)$.

(iv) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(I : J) = f^{-1}(I) : f^{-1}(J)$.

(v) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(\mathrm{Rad}(I)) = \mathrm{Rad}\big(f^{-1}(I)\big)$.

3-13. Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Υποτιθεμένου ότι $\chi\alpha\rho(R) > 0$, να αποδειχθεί ότι $\chi\alpha\rho(f(R)) \leq \chi\alpha\rho(R)$.

3-14. Να αποδειχθεί ότι ισόμορφοι δακτύλιοι έχουν ίσες χαρακτηριστικές.

3-15. Εάν R και R' είναι δυο δακτύλιοι με μοναδιαίο στοιχείο, να αποδειχθεί ότι δεν υφίστανται ομομορφισμοί $f : R \longrightarrow R'$ με $f(1_R) = 1_{R'}$ όταν ικανοποιείται μία εκ των κάτωθι συνθηκών:

(i) $\chi\alpha\rho(R) > 0 = \chi\alpha\rho(R')$.

(ii) $\chi\alpha\rho(R) > 0$, $\chi\alpha\rho(R') > 0$ και $\chi\alpha\rho(R') \nmid \chi\alpha\rho(R)$.

3-16. Εάν $f : K \longrightarrow L$ είναι ένας ομομορφισμός μεταξύ στρεβλών σωμάτων με $f(1_R) = 1_{R'}$, να αποδειχθεί ότι $\chi\alpha\rho(K) = \chi\alpha\rho(L)$.

3-17. Έστω $f : R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων. Να αποδειχθούν τα εξής:

(i) Ο R' είναι ακεραία περιοχή εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι πρώτο ιδεώδες τού R.

(ii) Ο R' είναι σώμα εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι μεγιστικό ιδεώδες τού R.

3-18. Να αποδειχθεί ότι δεν υφίστανται ομομορφισμοί $f : \mathbb{C} \longrightarrow S$ (από το σώμα των μιγαδικών αριθμών σε έναν δακτύλιο S) με $\mathrm{Ker}(f) = \mathbb{Z}$.

3-19. Να αποδειχθεί ότι $\mathbb{Z}[\sqrt{3}] \ncong \mathbb{Z}[\sqrt{5}]$ και $\mathbb{Z}[\mathrm{X}] \ncong \mathbb{Q}[\mathrm{X}]$.

3-20. Έστω $f : R \longrightarrow S$ ένας ισομορφισμός δακτυλίων με μοναδιαία στοιχεία. Να αποδειχθούν τα ακόλουθα:

(i) Έστω $r \in R$. Τότε $r \in R^{\times} \Leftrightarrow f(r) \in S^{\times}$.

(ii) Η απεικόνιση $R^{\times} \ni r \longmapsto f(r) \in S^{\times}$ είναι αμφιρριπτική.

3-21. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν υποτεθεί ότι κάθε υποδακτύλιος τού R είναι ιδεώδες, να αποδειχθεί ότι ο R είναι *είτε* τετριμμένος *είτε* ισόμορφος με τον δακτύλιο $\mathbb{Z}$ των ακεραίων *είτε* ισόμορφος με τον δακτύλιο $\mathbb{Z}_m$, όπου $m \in \mathbb{N}$, $m \geq 2$. [*Υπόδειξη*: Να χρησιμοποιηθεί ο ομομορφισμός δακτυλίων $f : \mathbb{Z} \longrightarrow R$, $n \longmapsto f(n) := n \cdot 1_R$, το 1ο θεώρημα ισομορφισμών 3.3.3 και η πρόταση 2.2.6.]

3-22. Έστω M ένα μη κενό σύνολο και έστω $(\mathfrak{P}(M), \triangle, \cap)$ ο δακτύλιος ο ορισθείς στην άσκηση **1-9**. Να αποδειχθούν τα ακόλουθα για οιοδήποτε $E \subseteq M$:

(i) Το $\mathfrak{P}(E)$ είναι ένα ιδεώδες τού $\mathfrak{P}(M)$.

(ii) Η απεικόνιση

$$f_E : \mathfrak{P}(M) \longrightarrow \mathfrak{P}(M), \quad A \longmapsto f_E(A) := A \cap (M \smallsetminus E)$$

είναι ομομορφισμός.

(iii) $\mathfrak{P}(M)/\mathfrak{P}(E) \cong \mathfrak{P}(M \smallsetminus E)$.

3-23. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο

$$S := \left\{ \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

αποτελεί έναν υποδακτύλιο τού $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

(ii) Η απεικόνιση $f : \mathbb{Z}[\sqrt{m}] \longrightarrow S$ η οριζόμενη από τον τύπο

$$\mathbb{Z}[\sqrt{m}] \ni a + b\sqrt{m} \overset{f}{\longmapsto} \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \in S$$

είναι ένας ισομορφισμός δακτυλίων. Ως εκ τούτου, ο S είναι μια ακεραία περιοχή. (Βλ. άσκηση **1-44** και το (i) τού πορίσματος 3.1.11.)

3-24. Να αποδειχθεί ότι $\mathbb{R}[\mathsf{X}]/\langle \mathsf{X}^2 \rangle \cong S$, όπου

$$S := \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \;\middle|\; a, b \in \mathbb{R} \right\}.$$

[*Υπόδειξη*: Να δειχθεί ότι η απεικόνιση

$$\mathbb{R}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto \left(\begin{array}{cc} a_0 & a_1 \\ 0 & a_0 \end{array} \right) \in S$$

είναι επιμορφισμός δακτυλίων έχων το κύριο ιδεώδες $\langle \mathsf{X}^2 \rangle$ ως πυρήνα του και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-25. Εάν $I := \langle \mathsf{X}^2 + 1 \rangle$ και $J := \langle \mathsf{X}^2 + 2 \rangle \subsetneq \mathbb{R}[\mathsf{X}]$, να αποδειχθεί ότι

$$\mathbb{R}[\mathsf{X}]/I \cong \mathbb{R}[\mathsf{X}]/J \;\text{ και }\; I \neq J.$$

3-26. Να αποδειχθούν τα ακόλουθα:

(i) Το ιδεώδες $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$ είναι πρώτο ιδεώδες τού $\mathbb{Z}[\mathsf{X}_1, \mathsf{X}_2]$ αλλά δεν είναι μεγιστικό.

(ii) Το ιδεώδες $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$ είναι μεγιστικό ιδεώδες τού $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$.

[*Υπόδειξη*: Εάν $R \in \{\mathbb{Z}, \mathbb{Q}\}$, να δειχθεί ότι η απεικόνιση

$$R[\mathsf{X}_1, \mathsf{X}_2] \ni \sum a_{ij} \mathsf{X}_1^i \mathsf{X}_2^j \longmapsto a_{00} \in R$$

είναι επιμορφισμός δακτυλίων έχων ως πυρήνα του το $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$. Κατόπιν τούτου, να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3 σε συνδυασμό με το θεώρημα 2.6.4 και το πόρισμα 2.6.5.]

(iii) Έστω τυχόν $\xi \in [0,1]$. Τότε το $\mathfrak{m}_\xi := \{ f \in \mathcal{C}([0,1]) \mid f(\xi) = 0 \}$ είναι ένα μεγιστικό ιδεώδες τού δακτυλίου

$$\mathcal{C}([0,1]) := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f \text{ συνεχής} \right\}$$

(βλ. άσκηση **1-37**). [*Υπόδειξη*: Να χρησιμοποιηθεί ο ομομορφισμός

$$\psi_\xi : \mathcal{C}([0,1]) \longrightarrow \mathbb{R}$$

ο οριζόμενος από τον τύπο $\psi_\xi(f) := f(\xi)$, καθώς και το 1ο θεώρημα ισομορφισμών 3.3.3.]

(iv) Ένα ιδεώδες I τού $\mathcal{C}([0,1])$ είναι μεγιστικό εάν και μόνον εάν $\exists \xi \in [0,1] : I = \mathfrak{m}_\xi$. [*Υπόδειξη*: Να γίνει κατάλληλη χρήση τής συμπάγειας τού κλειστού διαστήματος $[0,1]$.]

3-27. Έστω m ένας *θετικός* ακέραιος στερούμενος τετραγώνων και έστω

$$I_p(\sqrt{m}) := \left\{ a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \mid \text{με } p \mid a \text{ και } p \mid b \right\} \subsetneqq \mathbb{R},$$

όπου p περιττός πρώτος με $p \nmid m$. Να αποδειχθούν τα εξής:

(i) Το $I_p(\sqrt{m})$ είναι ένα ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$.

(ii) Εάν $n^2 \not\equiv m (\mathrm{mod}\, p)$, $\forall n \in \mathbb{Z}$, τότε το $I_p(\sqrt{m})$ είναι ένα μεγιστικό ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$ και ο πηλικοδακτύλιος $\mathbb{Z}[\sqrt{m}]/I_p(\sqrt{m})$ ένα σώμα με p^2 στοιχεία.

3-28. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R (όπου $n \in \mathbb{N},\ n \geq 2$), τότε το άθροισμά τους $I = I_1 + \cdots + I_n$ καλείται **(εσωτερικό) ευθύ άθροισμα**, σημειούμενο μέσω τού ειδικού συμβόλου $I_1 \oplus \cdots \oplus I_n$, όταν κάθε στοιχείο $a \in I$ εκφράζεται *μονοσημάντως* ως

$$a = a_1 + \cdots + a_n, \;\; a_j \in I_j, \;\; \forall j \in \{1, \ldots, n\}.$$

Να αποδειχθεί η ισοδυναμία των ακολούθων συνθηκών:

(i) Το I είναι το ευθύ άθροισμα των $I_1, \ldots, I_n$.

(ii) Εάν $0_R = a_1 + \cdots + a_n$, όπου $a_j \in I_j,\ \ \forall j \in \{1, \ldots, n\}$, τότε

$$a_1 = \cdots = a_n = 0_R.$$

(iii) $I_j \cap \big(\sum_{k \in \{1,\ldots,n\} \smallsetminus \{j\}} I_k \big) = \{0_R\},\ \ \forall j \in \{1, \ldots, n\}.$

3-29. Να αποδειχθούν τα ακόλουθα:

(i) Εάν $R = R_1 \times \cdots \times R_n$ είναι το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ (όπου $n \in \mathbb{N},\ n \geq 2$), και

$$\widetilde{R}_j := \left\{ \left(0_{R_1}, \ldots, 0_{R_{j-1}}, a_j, 0_{R_{j+1}} \ldots, 0_{R_n}\right) \in R \;\middle|\; a_j \in R_j \right\},$$

τότε $R = \widetilde{R}_1 \oplus \cdots \oplus \widetilde{R}_n$, όπου τα $\widetilde{R}_j$ και R_j είναι ισόμορφοι ως δακτύλιοι.

(ii) Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R (όπου $n \in \mathbb{N},\ n \geq 2$), και $R = I_1 \oplus \cdots \oplus I_n$, τότε

$$\boxed{R \cong I_1 \times \cdots \times I_n,}$$

με καθένα των $I_1, \ldots, I_n$ θεωρούμενο ως «αυτόνομος» δακτύλιος (ήτοι ως το «εξωτερικό» ευθύ γινόμενο των $I_1, \ldots, I_n$).

3-30. Έστω $R = R_1 \times \cdots \times R_n$ το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ με μοναδιαία στοιχεία (όπου $n \in \mathbb{N},\ n \geq 2$). Να αποδειχθούν τα εξής:

(i) Για κάθε $j \in \{1, \ldots, n\}$ η **φυσική προβολή** pr_j **τού** R **επί τού** R_j η οριζόμενη από τον τύπο

$$\mathrm{pr}_j : R \longrightarrow R_j,\ (a_1, \ldots, a_n) \longmapsto \mathrm{pr}_j(a_1, \ldots, a_n) := a_j,$$

είναι επιμορφισμός δακτυλίων.

(ii) Κάθε ιδεώδες I τού R είναι τής μορφής

$$\boxed{I = I_1 \oplus \cdots \oplus I_n \cong I_1 \times \cdots \times I_n,}$$

όπου I_j κάποιο ιδεώδες τού R_j, για κάθε $j \in \{1, \ldots, n\}$. [*Υπόδειξη*: Αρκεί να τεθεί $I_j := \mathrm{pr}_j(I)$.]

(iii) Ένα γνήσιο ιδεώδες I τού R είναι μεγιστικό εάν και μόνον εάν αυτό είναι τής μορφής

$$\begin{aligned} I &= R_1 \oplus \cdots \oplus R_{j-1} \times \mathfrak{m}_j \oplus R_{j+1} \oplus \cdots \oplus R_n \\ &\cong R_1 \times \cdots \times R_{j-1} \times \mathfrak{m}_j \times R_{j+1} \times \cdots \times R_n, \end{aligned}$$

όπου το $\mathfrak{m}_j$ είναι ένα μεγιστικό ιδεώδες τού R_j για κάποιον $j \in \{1, \ldots, n\}$.

3-31. Εάν τα I_1, I_2 είναι δυο ιδεώδη ενός δακτυλίου R και $R = I_1 \oplus I_2$, να αποδειχθεί ότι

$$R/I_1 \cong I_2 \ \text{ και } \ R/I_2 \cong I_1.$$

3-32. Έστω $R = R_1 \times \cdots \times R_n$ το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ (όπου $n \in \mathbb{N},\ n \geq 2$). Εάν το I_j είναι ένα ιδεώδες τού R_j για κάθε $j \in \{1, \ldots, n\}$ και $I := I_1 \oplus \cdots \oplus I_n$,να αποδειχθεί ότι

$$\boxed{R/I \cong (R_1/I_1) \oplus \cdots \oplus (R_n/I_n).}$$

[*Υπόδειξη*: Για κάθε $j \in \{1, \ldots, n\}$ να δειχθεί ότι η απεικόνιση

$$f : R \longrightarrow (R_1/I_1) \times \cdots \times (R_n/I_n) \cong (R_1/I_1) \oplus \cdots \oplus (R_n/I_n)$$
$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n) := (\pi_{I_1}^{R_1}(a_1), \ldots, \pi_{I_n}^{R_n}(a_n))$$

είναι επιμορφισμός δακτυλίων με πυρήνα $\mathrm{Ker}(f) = I$ και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-33. (i) Εάν οι R και S είναι δυο δακτύλιοι και $I = \{\,(r, 0_S) \mid r \in R\}$, να αποδειχθεί ότι το I είναι ιδεώδες τού $R \times S$ και ότι

$$(R \times S)\,/I \cong S.$$

(ii) Εάν $m, n \in \mathbb{N}$, να αποδειχθεί ότι

$$(\mathbb{Z} \times \mathbb{Z})\,/\,(m\mathbb{Z} \times n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

3-34. Έστω R ένας μεταθετικός δακτύλιος ο οποίος περιέχει ένα ταυτοδύναμο στοιχείο c. Εάν

$$I := \{\,a \in R \mid ac = 0_R\}\,,\ \ J := \{\,a \in R \mid ac = a\}\,,$$

να αποδειχθούν τα ακόλουθα:

(i) Τα I και J είναι ιδεώδη τού R.

(ii) $J = \langle c \rangle$.

(iii) $R \cong I \times J$.

(iv) $IJ = \{0_R\}$.

3-35. Έστω ότι ο R είναι ένας δακτύλιος, ο S ένας υποδακτύλιος τού R και το I ένα ιδεώδες τού R. Εάν $S \cap I = \{0_R\}$, να αποδειχθεί ότι ο S είναι ισόμορφος με έναν υποδακτύλιο τού πηλικοδακτυλίου R/I. [*Υπόδειξη*: Να χρησιμοποιηθεί το 2ο θεώρημα ισομορφισμών 3.3.16.]

3-36. Να προσδιορισθούν όλα τα πρώτα και τα μεγιστικά ιδεώδη τού δακτυλίου $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ (για οιονδήποτε $m \in \mathbb{N}$), καθώς και η τομή όλων των μεγιστικών ιδεωδών αυτού.

3-37. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω τυχόν $f(\mathsf{X}) \in R[\mathsf{X}]$. Εάν

$$\varphi(\mathsf{X}) = \sum\nolimits_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],$$

τότε μέσω τής απεικονίσεως

$$\mathfrak{v}_{\varphi(\mathsf{X})} : R \longrightarrow R, \quad r \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}(r) := \varphi(r) := \sum_{i=1}^{n} a_i r^i.$$

τής επαγομένης από το $\varphi(\mathsf{X})$ ορίζεται η απεικόνιση

$$R\,[\mathsf{X}] \longrightarrow \text{ΑΠ}\,(R, R) = R^R, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}.$$

καθώς και η **απεικόνιση πολυωνυμικής αποτιμήσεως σε ένα** (παγιωμένο) **στοιχείο** $r \in R$:

$$\boldsymbol{\varepsilon}_r : R\,[\mathsf{X}] \longrightarrow R, \quad \varphi(\mathsf{X}) \longmapsto \boldsymbol{\varepsilon}_r(\,\varphi(\mathsf{X})) := \mathfrak{v}_{\varphi(\mathsf{X})}(r) := \varphi(r)$$

(βλ. 1.3.11). Να αποδειχθούν τα ακόλουθα:

(i) Η $R\,[\mathsf{X}] \ni \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})} \in R^R$ είναι ομομορφισμός δακτυλίων και είναι, ιδιαιτέρως, επιμορφισμός όταν $R = \mathbb{Z}_p$, όπου p πρώτος αριθμός, ενώ δεν είναι επιμορφισμός όταν $R = \mathbb{R}$. [*Σημείωση*: Όπως έχει ήδη επισημανθεί στο εδάφιο 1.3.11, η $R\,[\mathsf{X}] \ni \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})} \in R^R$ δεν είναι κατ' ανάγκην μονομορφισμός και, ως εκ τούτου, ο $R\,[\mathsf{X}]$ δεν είναι πάντοτε εμφυτεύσιμος στον R^R.]

(ii) Η $\boldsymbol{\varepsilon}_r$ είναι επιμορφισμός για κάθε $r \in R$.

3-38. Δοθέντος ενός ομομορφισμού $f : R \longrightarrow S$ μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, να αποδειχθεί ότι οι απεικονίσεις

$$\theta_f^{(1)} : R[\mathsf{X}] \longrightarrow S[\mathsf{X}], \qquad \theta_f^{(2)} : R[\![\mathsf{X}]\!] \longrightarrow S[\![\mathsf{X}]\!],$$
$$\theta_f^{(3)} : R[\mathsf{X}^{\pm 1}] \longrightarrow S[\mathsf{X}^{\pm 1}], \quad \theta_f^{(4)} : \text{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \longrightarrow \text{Laur}_S[\![\mathsf{X}^{\pm 1}]\!],$$

οι οριζόμενες μέσω των τύπων

$$R[\mathsf{X}] \ni \textstyle\sum_{i=0}^{n} a_i \mathsf{X}^i \overset{\theta_f^{(1)}}{\longmapsto} \sum_{i=0}^{n} f(a_i)\mathsf{X}^i \in S[\mathsf{X}],\ n \in \mathbb{N}_0,$$

$$R[\![\mathsf{X}]\!] \ni \textstyle\sum_{i=0}^{\infty} a_i \mathsf{X}^i \overset{\theta_f^{(2)}}{\longmapsto} \sum_{i=0}^{\infty} f(a_i)\mathsf{X}^i \in S[\![\mathsf{X}]\!],$$

$$R[\mathsf{X}^{\pm 1}] \ni \textstyle\sum_{i=-n}^{m} a_i \mathsf{X}^i \overset{\theta_f^{(3)}}{\longmapsto} \sum_{i=-n}^{m} f(a_i)\mathsf{X}^i \in S[\mathsf{X}^{\pm 1}],\ m, n \in \mathbb{N},$$

$$\text{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \ni \textstyle\sum_{i=-n}^{\infty} a_i \mathsf{X}^i \overset{\theta_f^{(4)}}{\longmapsto} \sum_{i=-n}^{\infty} f(a_i)\mathsf{X}^i \in \text{Laur}_S[\![\mathsf{X}^{\pm 1}]\!],\ n \in \mathbb{N},$$

είναι ομομορφισμοί δακτυλίων με $\theta_f^{(j)}(1_R) = 1_S$ και να προσδιορισθούν οι πυρήνες $\mathrm{Ker}(\theta_f^{(j)})$ για κάθε $j \in \{1,2,3,4\}$ (βλ. 1.3.1 και άσκηση **1-52**). Εν συνεχεία, να επαληθευθούν για κάθε $j \in \{1,2,3,4\}$ οι ακόλουθες αμφίπλευρες συνεπαγωγές:

(i) Η $\theta_f^{(j)}$ είναι μονομορφισμός $\Leftrightarrow$ ο f είναι μονομορφισμός.

(ii) Η $\theta_f^{(j)}$ είναι επιμορφισμός $\Leftrightarrow$ ο f είναι επιμορφισμός.

3-39. Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω

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

Να αποδειχθεί η ακόλουθη αμφίπλευρη συνεπαγωγή (η οποία γενικεύει το πρώτο αποτέλεσμα τού (iii) τής προτάσεως 1.3.9 που περιγράφει την ομάδα $R[\mathsf{X}]^\times$ στην ειδική περίπτωση όπου ο R είναι *ακεραία περιοχή*):

$$\varphi(\mathsf{X}) \in R[\mathsf{X}]^\times \iff a_0 \in R^\times \ \text{ και } \ a_j \in \mathrm{Nil}(R),\ \forall j \in \{1,\dots,n\}.$$

[*Υπόδειξη*: Για την κατεύθυνση "$\Leftarrow$" να χρησιμοποιηθούν οι ασκήσεις **2-6** και **1-28**. Για την απόδειξη τής συνεπαγωγής "$\Rightarrow$" να αποδειχθεί απευθείας ότι $a_0 \in R^\times$ και να θεωρηθεί *τυχόν* πρώτο ιδεώδες $\mathfrak{p}$ τού R, ο φυσικός επιμορφισμός $\pi_{\mathfrak{p}}^R : R \longrightarrow R/\mathfrak{p}$ και ο επαγόμενος επιμορφισμός

$$\theta^{(1)}_{\pi_{\mathfrak{p}}^R} : R[\mathsf{X}] \longrightarrow (R/\mathfrak{p})[\mathsf{X}] \ \text{ με } \ \theta^{(1)}_{\pi_{\mathfrak{p}}^R}(1_R) = 1_{R/\mathfrak{p}} = 1_R + \mathfrak{p}.$$

(Βλ. άσκηση **3-38**.) Σύμφωνα με το θεώρημα 2.6.4 ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή. Ως εκ τούτου, ο $(R/\mathfrak{p})[\mathsf{X}]$ είναι ωσαύτως ακεραία περιοχή (βλ. 1.3.9 (i)). Κατά το (viii) τής προτάσεως 3.1.5,

$$\sum_{i=0}^{n} \pi_{\mathfrak{p}}^R(a_i)\mathsf{X}^i \in ((R/\mathfrak{p})[\mathsf{X}])^\times,$$

οπότε εφαρμόζοντας γι' αυτό το πολυώνυμο το πρώτο αποτέλεσμα τού (iii) τής προτάσεως 1.3.9 λαμβάνουμε

$$\pi_{\mathfrak{p}}^R(a_0) \in ((R/\mathfrak{p})[\mathsf{X}])^\times, \ \ \pi_{\mathfrak{p}}^R(a_j) = 0_{R/\mathfrak{p}} = \mathfrak{p},\ \forall j \in \{1,\dots,n\}.$$

Από τις τελευταίες ισότητες έπεται ότι $a_j \in \mathfrak{p},\ \forall j \in \{1,\dots,n\}$. Επειδή το $\mathfrak{p}$ είναι αυθαιρέτως επιλεγμένο πρώτο ιδεώδες τού R, συμπεραίνουμε τελικώς ότι

$$a_j \in \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(R)\} = \mathrm{Nil}(R),\ \forall j \in \{1,\dots,n\},$$

κάνοντας χρήση τού (ii) τής ασκήσεως **2-37**.]

3-40. Να αποδειχθεί ότι για οιονδήποτε δακτύλιο R και οιονδήποτε $n \in \mathbb{N}$ η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R^{\mathrm{opp}}) \ni \mathbf{A} \longmapsto \mathbf{A}^{\intercal} \in (\mathrm{Mat}_{n\times n}(R))^{\mathrm{opp}}$$

είναι ισομορφισμός, όπου R^{opp} είναι ο δακτύλιος ο αντικείμενος τού R (βλ. άσκηση **1-4**) και $\mathbf{A}^{\intercal}$ ο *ανάστροφος* τού πίνακα $\mathbf{A}$ (που προκύπτει από τον $\mathbf{A}$ όταν καθιστούμε τις γραμμές του στήλες (και τις στήλες του γραμμές)).

3-41. Να αποδειχθεί ότι για οιονδήποτε δακτύλιο R με μοναδιαίο στοιχείο και οιονδήποτε $n \in \mathbb{N}$ υφίστανται κανονιστικοί ισομορφισμοί

$$\boxed{\mathrm{Mat}_{n\times n}(R)[\mathsf{X}] \cong \mathrm{Mat}_{n\times n}(R[\mathsf{X}])} \quad \text{και} \quad \boxed{\mathrm{Mat}_{n\times n}(R)[\![\mathsf{X}]\!] \cong \mathrm{Mat}_{n\times n}(R[\![\mathsf{X}]\!]).}$$

3-42. Δοθέντος ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ και ενός $n \in \mathbb{N}$ να αποδειχθεί ότι η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R) \ni (a_{jk})_{1\le j,k\le n} \overset{\mathrm{Mat}_{n\times n}(f)}{\longmapsto} (f(a_{jk}))_{1\le j,k\le n} \in \mathrm{Mat}_{n\times n}(S),$$

είναι ομομορφισμός δακτυλίων και έχει τις εξής ιδιότητες:

(i) Η $\mathrm{Mat}_{n\times n}(f)$ είναι μονομορφισμός $\Leftrightarrow$ ο f είναι μονομορφισμός.

(ii) Η $\mathrm{Mat}_{n\times n}(f)$ είναι επιμορφισμός $\Leftrightarrow$ ο f είναι επιμορφισμός.

3-43. Έστω I ένα ιδεώδες ενός δακτυλίου R. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$ υφίσταται κανονιστικός ισομορφισμός δακτυλίων

$$\boxed{\mathrm{Mat}_{n\times n}(R) \,/\, \mathrm{Mat}_{n\times n}(I) \cong \mathrm{Mat}_{n\times n}(R/I)}$$

[*Υπόδειξη*: Να αποδειχθεί ότι ο επιμορφισμός

$$\mathrm{Mat}_{n\times n}(\pi_I^R) : \mathrm{Mat}_{n\times n}(R) \longrightarrow \mathrm{Mat}_{n\times n}(R/I)$$

(ο ορισθείς στην άσκηση **3-42**) έχει ως πυρήνα του το ιδεώδες $\mathrm{Mat}_{n\times n}(I)$ και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-44. Έστω R τυχών δακτύλιος και έστω n ένας φυσικός αριθμός ≥ 2. Για κάθε n-άδα $(r_1, \ldots, r_n) \in R^n$ σημειώνουμε ως $\mathrm{diag}(r_1, \ldots, r_n)$ τον *διαγώνιο πίνακα* $(a_{jk})_{1\le j,k\le n} \in \mathrm{Mat}_{n\times n}(R)$ με εγγραφές τις

$$a_{jk} := \begin{cases} r_j, & \text{όταν } j = k, \\ 0_R, & \text{όταν } j \neq k. \end{cases}$$

(i) Να αποδειχθεί ότι το σύνολο των διαγωνίων πινάκων

$$\mathrm{Diag}_n(R) := \{\, \mathrm{diag}(r_1, \ldots, r_n) \mid (r_1, \ldots, r_n) \in R^n \}$$

είναι ένας υποδακτύλιος τού $\mathrm{Mat}_{n\times n}(R)$ που είναι ισόμορφος με τον R^n.

(ii) Σύμφωνα με την άσκηση **2-18**, ο $\mathrm{SUT}_n(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{UT}_n(R)$ και ο $\mathrm{LUT}_n(R)$ ένα ιδεώδες τού δακτυλίου $\mathrm{LT}_n(R)$. Να αποδειχθεί ότι

$$\mathrm{UT}_n(R)/\mathrm{SUT}_n(R) \cong \mathrm{Diag}_n(R) \cong \mathrm{LT}_n(R)/\mathrm{LUT}_n(R).$$

3-45. Να προσδιορισθούν όλα τα ιδεώδη τού δακτυλίου $\mathrm{Mat}_{n\times n}(\mathbb{Z}_{12})$ $(n \in \mathbb{N})$. [*Υπόδειξη*: Να χρησιμοποιηθεί το εδάφιο 3.2.6 σε συνδυασμό με το (vi) τής ασκήσεως **2-16**.]

3-46. Να προσδιορισθούν τα σύνολα λύσεων των συστημάτων γραμμικών ισοτιμιών:

$$\left\{\begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{array}\right\}$$

και

$$\left\{\begin{array}{l} 5x \equiv 6 \pmod 8 \\ 8x \equiv 10 \pmod{14} \\ 10x \equiv 5 \pmod{15} \end{array}\right\}$$

βάσει των τεχνικών που παρετέθησαν στην ενότητα 3.4.

3-47. Έστω m ένας ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθεί ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{m}]) = \mathbb{Q}(\sqrt{m})$. [*Υπόδειξη*: Να γενικευθούν καταλλήλως τα προαναφερθέντα στο παράδειγμα 3.5.10.]

3-48. Έστω R μια ακεραία περιοχή. Να αποδειχθεί ότι $\mathrm{χαρ}(\mathbf{Fr}(R)) = \mathrm{χαρ}(R)$.

3-49. Να αποδειχθούν τα ακόλουθα:

(i) Έστω K ένα σώμα και έστω K_0 το (μοναδικό) πρώτο υπόσωμα τού K (βλ. θεώρημα 3.6.3). Εάν ο $f : K \longrightarrow K$ είναι ένας αυτομορφισμός τού K, τότε

$$f(a) = a,\ \forall a \in K_0.$$

Εξ αυτού έπεται, ειδικότερα, ότι η ταυτοτική απεικόνιση είναι ο μόνος αυτομορφισμός ενός πρώτου σώματος. [*Υπόδειξη*: Να χρησιμοποιηθεί η παρατήρηση 3.6.6.]

(ii) Δεν υπάρχουν άλλοι αυτομορφισμοί τού σώματος $\mathbb{R}$ των πραγματικών αριθμών πέραν τού ταυτοτικού. [*Υπόδειξη*: Είναι εύκολος ο έλεγχος τού ότι κάθε αυτομορφισμός $f : \mathbb{R} \longrightarrow \mathbb{R}$ τού $\mathbb{R}$ έχει την ιδιότητα: $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ (βάσει τού (i)) και διατηρεί τη συνήθη διάταξη τού $\mathbb{R}$. Να χρησιμοποιηθεί το

γεγονός ότι κάθε πραγματικός αριθμός είναι το όριο μιας (συγκλίνουσας) ακολουθίας ρητών αριθμών.]

(iii) Το (ii) δεν είναι αληθές για το σώμα $\mathbb{C}$ και για το στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$. (Αρκεί η παράθεση ενός μη ταυτοτικού αυτομορφισμού για καθέναν εξ αυτών.)

3-50. Έστω R μια ακεραία περιοχή και έστω $\mathfrak{p} \in \mathrm{Spec}(R)$. Το

$$\boxed{R_{\mathfrak{p}} := \left\{ \tfrac{a}{b} \in \mathbf{Fr}(R) \,\middle|\, a \in R, b \in R \smallsetminus \mathfrak{p} \right\}}$$

καλείται **τοπικοποίηση τού R στο $\mathfrak{p}$**. Να αποδειχθούν τα εξής:

(i) Το $R_{\mathfrak{p}}$ είναι ένας υποδακτύλιος τού σώματος $\mathbf{Fr}(R)$ περιέχων τον R.

(ii) $\mathbf{Fr}(R) \cong \mathbf{Fr}(R_{\mathfrak{p}})$.

(iii) Ο $R_{\mathfrak{p}}$ είναι τοπικός δακτύλιος έχων το $\mathfrak{m}_{R_{\mathfrak{p}}} := \mathfrak{p}R_{\mathfrak{p}}$ ως το (μοναδικό) μεγιστικό του ιδεώδες.

(iv) $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \mathbf{Fr}(R/\mathfrak{p})$.

(v) Όταν $R = \mathbb{Z}$ και $\mathfrak{p} = \langle p \rangle = p\mathbb{Z}$, όπου p κάποιος πρώτος αριθμός, ο $R_{\mathfrak{p}}$ είναι ο δακτύλιος των p-αδικών κλασμάτων $\mathbb{Z}_{\langle p \rangle}$ ο ορισθείς στην άσκηση **1-16** (σελ. 35) με

$$\mathfrak{m}_{\mathbb{Z}_{\langle p \rangle}} = p\mathbb{Z}_{\langle p \rangle} = \mathbb{Z}_{\langle p \rangle} \smallsetminus \mathbb{Z}_{\langle p \rangle}^{\times} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; \text{μκδ}\,(a,b) = 1 \text{ και } p \nmid b,\ p \mid a \right\}$$

(πρβλ. 2.7.3 (ii)) και $\mathbb{Z}_{\langle p \rangle}/p\mathbb{Z}_{\langle p \rangle} \cong \mathbb{Z}_p$.