ΚΕΦΑΛΑΙΟ 4

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. 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.

4.1 ΔΑΚΤΥΛΙΟΙ ΚΑΙ ΥΠΟΔΑΚΤΥΛΙΟΙ

4.1.1 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) για κάθε a, b και $c \in R$ να ισχύει τόσο ο *αριστερός* όσο και ο *δεξιός επιμεριστικός νόμος*, ήτοι

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

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

4.1.2 Παρατήρηση. 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 4.1.1 χωρίς όμως και να τη σημειώνουμε. Επίσης, εάν $n \in \mathbb{N}$ και τα $a_1, \ldots, a_n$ είναι στοιχεία ενός δακτυλίου R, τότε χρησιμοποιούμε ενίοτε τις βραχυγραφίες

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

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

4.1.4 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 1-δακτυλίων.

(ii) Εάν $n \in \mathbb{N}$ και το $(R, +, \cdot)$ ένας δακτύλιος, τότε το σύνολο $\mathrm{Mat}_{n\times n}(R)$ όλων των $(n \times n)$-πινάκων με εγγραφές ειλημμένες από το R (βλ. 3.1.6) καθίσταται δακτύλιος μέσω τής προσθετικής πράξεως

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

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 είναι ένας εκ των $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$, τότε προφανώς ο $\mathrm{Mat}_{n\times n}(R)$ δεν είναι μεταθετικός στην περίπτωση κατά την οποία $n > 1$. (Οι έννοιες: *υποπίνακας πίνακα*, *γραμμές/στήλες πίνακα*, *ελάσσονες πίνακες* κλπ. ορίζονται όπως και στη συνήθη Γραμμική Άλγεβρα. Για την εμπέδωση των απαραίτητων ιδιοτήτων των *οριζουσών πινάκων* που ανήκουν στον $\mathrm{Mat}_{n\times n}(R)$ παροτρύνουμε τον αναγνώστη, στο σημείο αυτό, να επιλύσει την άσκηση ??).

(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. Το σύνολο

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

όλων των κλάσεων υπολοίπων κατά μόδιο m (βλ. 2.4.24), εφοδιασμένο με τις πράξεις προσθέσεως και πολλαπλασιασμού τις ορισθείσες στο θεώρημα 1.7.8, αποτελεί έναν μεταθετικό 1-δακτύλιο.

(v) Έστω X ένα μη κενό σύνολο και R ένας 1-δακτύλιος. Τότε το σύνολο των απεικονίσεων $R^X := \{\text{απεικονίσεις } f : X \longrightarrow R\}$ καθίσταται ένας 1-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 $X = \{1, \ldots, n\} \subset \mathbb{N}$, 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 προσλαμβάνει τη δομή τού δακτυλίου μέσω των πράξεων

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

με ουδέτερο στοιχείο ως προς την πρόσθεση το $(0_R, \ldots, 0_R)$ και με μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό το $(1_R, \ldots, 0_R)$. Εξάλλου, δοθέντων n αυθαιρέτως επιλεγμένων 1-δακτυλίων $R_1, R_2, \ldots, R_n$, μπορούμε να ορίσουμε τη δομή ενός

1-δακτυλίου επί τού *καρτεσιανού* (ή *ευθέος*) *γινομένου* τους

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

με τις ανάλογες πράξεις κατά παράγοντες. Κατ' αναλογίαν, εάν η $(R_j)_{j\in J}$ είναι μια μη κενή οικογένεια 1-δακτυλίων, μπορούμε να ορίσουμε τη δομή ενός 1-δακτυλίου επί τού $\prod_{j\in J} R_j$ μέσω των πράξεων

$$\begin{aligned}(x_j)_{j\in J} + (y_j)_{j\in J} &= (x_j + y_j)_{j\in J},\\ (x_j)_{j\in J} \cdot (y_j)_{j\in J} &= (x_j \cdot y_j)_{j\in J},\end{aligned}$$

και με το $(1_{R_j})_{j\in J}$ ως μοναδιαίο του στοιχείο.

(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 1-δακτύλιο $(\mathbb{Z}, \boxplus, \boxdot)$ 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

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

(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.

4.1.5 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 οιαδήποτε στοιχεία* $a_1, \ldots, a_n, b_1, \ldots, b_m$ *τού* R *έχουμε*

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

(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 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 επί τού 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, $R\smallsetminus\{0_R\} \neq \varnothing$. Άρα, για κάθε $a \in R\smallsetminus\{0_R\}$, έχουμε $1_R a = a$, οπότε $1_R \neq 0_R$. □

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

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

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.

4.1.7 Πρόταση. (Διωνυμικοί τύποι) *Για κάθε μη αρνητικό ακέραιο αριθμό n ας συμβολίσουμε ως $n! = 1 \cdot 2 \cdots n$ 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 1-δακτύλιος, 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*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k} \tag{4.1}$$

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

$$(a_1 + a_2 + \cdots + a_\nu)^n = \sum \frac{n!}{(i_1!)\,(i_2!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2}\, \cdots\, a_\nu^{i_\nu} \tag{4.2}$$

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:

$$\tbinom{n}{j} + \tbinom{n}{j+1} = \tbinom{n+1}{j+1} \tag{4.3}$$

για κάθε $j, 0 \leq j < n$, και θα εργασθούμε με μαθηματική επαγωγή επί τού n. Για $n = 0$ η (4.1) είναι προφανής. Υποθέτοντας ότι η (4.1) είναι αληθής για κάποιον $n \geq 1$, λαμβάνουμε μέσω τής επιμεριστικής ιδιότητας:

$$\begin{aligned}
&(a+b)^{n+1} = (a+b)\sum_{k=0}^{n}\tbinom{n}{k}\,a^k\,b^{n-k}\\
&=\sum_{k=0}^{n}\tbinom{n}{k}\,a^{k+1}\,b^{n-k}+\sum_{k=0}^{n}\tbinom{n}{k}\,a^k\,b^{n-k+1}\quad[\text{επειδή } ab=ba]\\
&=\tbinom{n}{n}\,a^{n+1}+\sum_{k=0}^{n-1}\tbinom{n}{k}\,a^{k+1}\,b^{n-k}+\sum_{k=1}^{n}\tbinom{n}{k}\,a^k\,b^{n-k+1}+\tbinom{n}{0}\,b^{n+1}\\
&=\tbinom{n+1}{n+1}\,a^{n+1}+\sum_{j=0}^{n-1}\tbinom{n}{j}\,a^{j+1}\,b^{(n+1)-(j+1)}+\\
&+\sum_{j=0}^{n-1}\tbinom{n}{j+1}\,a^{j+1}\,b^{(n+1)-(j+1)}+\tbinom{n+1}{0}\,b^{n+1}\\
&=\tbinom{n+1}{n+1}\,a^{n+1}+\sum_{j=0}^{n-1}\left(\tbinom{n}{j}+\tbinom{n}{j+1}\right)\,a^{j+1}\,b^{(n+1)-(j+1)}+\tbinom{n+1}{0}\,b^{n+1}\\
&\overset{(4.3)}{=}\tbinom{n+1}{n+1}\,a^{n+1}+\sum_{j=0}^{n-1}\tbinom{n+1}{j+1}\,a^{j+1}\,b^{(n+1)-(j+1)}+\tbinom{n+1}{0}\,b^{n+1}\\
&=\tbinom{n+1}{n+1}\,a^{n+1}+\sum_{k=0}^{n}\tbinom{n+1}{k}\,a^k\,b^{(n+1)-k}+\tbinom{n+1}{0}\,b^{n+1}=\sum_{k=0}^{n+1}\tbinom{n+1}{k}\,a^k\,b^{(n+1)-k}\,.
\end{aligned}$$

(ii) Για την απόδειξη τού τύπου (4.2) αρκεί να εφαρμόσουμε μαθηματική επαγωγή επί τού πληθικού αριθμού ν των προσθετέων. Για $n \in \{0,1\}$ ο (4.2) είναι προφανής, ενώ για $n = 2$ συμπίπτει με τον (4.1), αφού

$$(a_1+a_2)^n=\sum_{k=0}^{n}\tbinom{n}{k}\,a_1^k\,a_2^{n-k}=\sum_{k+j=n}\tfrac{n!}{k!\,j!}\,a_1^k\,a_2^j\,.$$

Εάν υποθέσουμε ότι ο (4.2) είναι αληθής για κάποιον ν, τότε θα είναι αληθής και για τον $\nu+1$, διότι

$$(a_1+a_2+\cdots+a_{\nu+1})^n=((a_1+a_2+\cdots+a_\nu)+a_{\nu+1})^n$$

$$=\sum_{k=0}^{n}\tbinom{n}{k}\,(a_1+a_2+\cdots+a_\nu)^k\,a_{\nu+1}^{n-k}=\sum_{k+j=n}\tfrac{n!}{k!\,j!}\,(a_1+a_2+\cdots+a_\nu)^k\,a_{\nu+1}^j\,,$$

πράγμα που μας οδηγεί στην απαιτούμενη ισότητα ύστερα από την αντικατάσταση τού αντιστοίχου τύπου για τους ν προσθετέους, την εφαρμογή τής ανά ζεύγη ισχύουσας μεταθετικής ιδιότητας, και την εκτέλεση των πράξεων. □

4.1.8 Σημείωση. Δεδομένων των συνθηκών αμοιβαίας μεταθετικότητας των όρων μας, ανεπαίσθητες παραλλαγές των (4.1) και (4.2) παραμένουν ισχύουσες ακόμη και όταν ο δακτύλιος R *δεν* διαθέτει μοναδιαίο στοιχείο. Συγκεκριμένα, όταν ο R δεν είναι 1-δακτύλιος, μπορούμε να γράψουμε αντί τής (4.1),

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

(και, αντιστοίχως, να μην εμφανίσουμε *καθόλου* στην (4.2) 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

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

4.1.9 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 "$\cdot$" (βλ. 1.5.2) και καθίσταται αφ' εαυτού δακτύλιος (ως προς τον περιορισμό των εν λόγω πράξεων επ' αυτού).

4.1.10 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* $a, b \in S$.

ΑΠΟΔΕΙΞΗ. Προφανώς, ένα $\varnothing \neq S \subseteq R$ είναι υποδακτύλιος εάν και μόνον εάν η προσθετική ομάδα $(S, +)$ είναι μια υποομάδα τής $(R, +)$ και το S είναι κλειστό ως προς την "$\cdot$". Άρα η απόδειξη έπεται άμεσα κάνοντας χρήση τής αμφίπλευρης συνεπαγωγής (i)$\Leftrightarrow$(iii) τής προτάσεως 3.2.15 και τής παρατηρήσεως 3.2.16. □

4.1.11 Παραδείγματα. (i) Ο δακτύλιος των ακεραίων είναι υποδακτύλιος τού $\mathbb{Q}$, ο $\mathbb{Q}$ είναι υποδακτύλιος τού $\mathbb{R}$ και ο $\mathbb{R}$ είναι υποδακτύλιος τού $\mathbb{C}$. Επίσης ο $2\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Z}$.

(ii) Ο **δακτύλιος των ακεραίων τού Gauss**

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

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

$$\boxed{\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \subsetneqq \mathbb{C}} \tag{4.4}$$

όπου $m \in \mathbb{Z} \smallsetminus \{0\}$, 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

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

Κατ' αναλογίαν, για κάθε $m \in \mathbb{Z} \smallsetminus \{0\}$, το

$$\boxed{\mathbb{Q}(\sqrt{m}) := \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \subsetneqq \mathbb{C}} \tag{4.5}$$

καθίσταται υποδακτύλιος τού $\mathbb{R}$, όταν $m \in \mathbb{N}$, και υποδακτύλιος τού $\mathbb{C}$, όταν έχουμε $m \in \mathbb{Z} \smallsetminus \mathbb{N}_0$. Σημειωτέον ότι ισχύουν οι ακόλουθοι εγκλεισμοί δακτυλίων:

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

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

4.1.12 Σημείωση. Υπάρχουν υποδακτύλιοι S δακτυλίων R που συμπεριφέρονται αρκετά παράξενα σε ό,τι 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 $(1, 0)$.

4.1.13 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 $0_R \in \bigcap_{j\in J} S_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $a, b \in \bigcap_{j\in J} S_j$, 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

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

Άρα η $\bigcap_{j\in J} S_j$ είναι όντως ένας υποδακτύλιος τού R (βλ. πρόταση 4.1.10). □

4.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

4.2.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα στοιχείο $a \in R\setminus\{0_R\}$ λέγεται *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 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 $\mathrm{Zdv}(R)$.

4.2.2 Παράδειγμα. Στον δακτύλιο $\mathrm{Mat}_{2\times 2}(R)$, όπου το R είναι ένας εκ των $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, έχουμε

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

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

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

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

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

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

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

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

" $\subseteq$ " Αυτό θα προκύψει άμεσα από το 3.2.7 (iii) και την κάπως γενικότερη πρόταση 4.2.12. □

4.2.5 Πρόταση. (Νόμος διαγραφής) *Ένας δακτύλιος 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*:

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

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 κανόνα 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 $cd = 0_R = c\ (0_R)$, οπότε από τον κανόνα τής διαγραφής λαμβάνουμε $d = 0_R$, ενώ εάν $d \neq 0_R$, τότε η $cd = 0_R = (0_R)\ d$ μας δίνει (κατ' αναλογίαν) $c = 0_R$. □

4.2.6 Ορισμός. Έστω R ένας 1-δακτύλιος με $1_R \neq 0_R$. Ένα στοιχείο $a \in R$ λέγεται **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** 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 1-δακτυλίου R με $1_R \neq 0_R$ θα συμβολίζεται ως $R^\times$.

4.2.7 Ορισμός. Κατά την πρόταση 3.2.6 το ζεύγος $(R^\times, \cdot)$ αποτελεί μια πολλαπλασιαστική ομάδα· αυτή καλείται, ιδιαιτέρως, **ομάδα των αντιστρεψίμων στοιχείων** τού δακτυλίου R.

4.2.8 Σημείωση. (i) Η $R^\times$ είναι δυνατόν να είναι αβελιανή ακόμη και όταν ο R δεν είναι μεταθετικός, πρβλ. άσκηση ??).

(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 $|\mathbb{Z}_m^\times| = \varphi(m)$, όπου φ η συνάρτηση τού Euler (βλ. 2.4.16 και 3.2.7 (iii)), και άλλοτε *άπειρη*. Επί παραδείγματι, η

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

είναι άπειρη αριθμήσιμη και η $(\text{Mat}_{n\times n}(\mathbb{R}))^\times$ άπειρη υπεραριθμήσιμη (βλ. πρόταση 4.2.9).

4.2.9 Πρόταση. *Εάν $n \in \mathbb{N}$ και ο R είναι ένας μεταθετικός μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, τότε για τον δακτύλιο* $\text{Mat}(n\times n; R)$ *των $n\times n$ πινάκων με τις εγγραφές τους ειλημμένες από τον R έχουμε*

$$\boxed{(\text{Mat}_{n\times n}(R))^\times = \{\text{οι πίνακες} \quad \mathbf{A} \in \text{Mat}_{n\times n}(R) \mid \det(\mathbf{A}) \in R^\times\}}$$

όπου ως $\det(\mathbf{A})$ *συμβολίζουμε την ορίζουσα τού* $\mathbf{A} \in \text{Mat}_{n\times n}(R)$.

ΑΠΟΔΕΙΞΗ. Εάν $\mathbf{A} \in (\text{Mat}_{n\times n}(R))^\times$, τότε υπάρχουν στοιχεία $\mathbf{B}, \mathbf{C}$ τού δακτυλίου $\text{Mat}_{n\times n}(R)$, τέτοια ώστε

$$\mathbf{AB} = \mathbf{CA} = \mathbf{I}_n.$$

Λαμβάνοντας υπ' όψιν τις ιδιότητες των οριζουσών $n\times n$ πινάκων με τις εγγραφές τους ειλημμένες από τον R, έχουμε

$$\det(\mathbf{AB}) = \det(\mathbf{A})\cdot\det(\mathbf{B}) = 1_R = \det(\mathbf{CA}) = \det(\mathbf{C})\cdot\det(\mathbf{A}),$$

δηλαδή ότι $\det(\mathbf{A}) \in R^\times$. Και αντιστρόφως· εάν $\mathbf{A} \in \text{Mat}_{n\times n}(R)$ με ορίζουσα $\delta := \det(\mathbf{A}) \in R^\times$, τότε από τη μεταθετικότητα τού R έχουμε $a\mathbf{C} = \mathbf{C}a$ για κάθε $a \in R$ και κάθε $\mathbf{C} \in \text{Mat}_{n\times n}(R)$, και επομένως και

$$\delta^{-1}(\mathbf{adj}(\mathbf{A})) = (\mathbf{adj}(\mathbf{A}))\delta^{-1},$$

όπου $\mathbf{adj}(\mathbf{A})$ ο πίνακας ο προσαρτημένος στον $\mathbf{A}$. Επειδή

$$\det(\mathbf{A})\ \mathbf{I}_n = \mathbf{A}\,(\mathbf{adj}(\mathbf{A})) = \mathbf{adj}(\mathbf{A})\ \mathbf{A},$$

λαμβάνουμε τελικώς

$$\mathbf{A}\,(\mathbf{adj}(\mathbf{A}))\delta^{-1} = \delta\delta^{-1}\,\mathbf{I}_n = \mathbf{I}_n = \delta^{-1}(\mathbf{adj}(\mathbf{A}))\mathbf{A},$$

οπότε $\mathbf{A} \in (\text{Mat}_{n\times n}(R))^\times$. □

4.2.10 Σημείωση. (i) Η ομάδα $(\mathrm{Mat}_{n\times n}(R))^{\times}$ συνήθως συμβολίζεται με το $\mathbf{GL}(n;R)$ και λέγεται **γενική γραμμική ομάδα** οριζόμενη υπεράνω τού R.

(ii) Εάν $\mathbf{A}\in(\mathrm{Mat}_{n\times n}(R))^{\times}$, τότε προφανώς το αντίστροφό του στοιχείο $\mathbf{A}^{-1}$ (το οποίο καλείται, ιδιαιτέρως, **αντίστροφος πίνακας τού A**) ισούται με

$$\mathbf{A}^{-1}=\det(\mathbf{A})^{-1}\,\mathbf{adj}(\mathbf{A})\,.$$

4.2.11 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 $\mathrm{Nil}(R)$.

4.2.12 Πρόταση. *Για κάθε 1-δακτύλιο R με $1_R\neq 0_R$ 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. Εάν $a\in\mathrm{Nil}(R)\smallsetminus\{0_R\}$, τότε έχουμε

$$a^n=a^{n-1}a=a\,a^{n-1}=0_R$$

για κάποιον $n\in\mathbb{N}$, οπότε $a\in\mathrm{Zdv}(R)$. 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 έχουμε $\mathrm{Zdv}(R)\cap R^{\times}=\varnothing$. Οι υπόλοιπες εγκλειστικές σχέσεις είναι προφανείς. □

4.2.13 Ορισμός. (i) Κάθε μεταθετικός 1-δακτύλιος R με $1_R\neq 0_R$ και $\mathrm{Zdv}(R)=\varnothing$ καλείται **ακεραία περιοχή.**

(ii) Κάθε 1-δακτύλιος R με $1_R\neq 0_R$ και $R^{\times}=R\smallsetminus\{0_R\}$ καλείται **διαιρετικός**[3] **δακτύλιος** ή **στρεβλό σώμα**[4]**.**

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

[3] 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 $b\in R\smallsetminus\{0_R\}$.

[4] 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 $0_R(\neq 1_R)$).

4.2.14 Παραδείγματα. (i) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ αποτελούν σώματα. Από την άλλη μεριά, όπως είδαμε στα 4.1.4 (ii) και 4.2.2, 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 $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ ο οριζόμενος μέσω των πραγματικών γραμμικών συνδυασμών των τεσσάρων πινάκων

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

και[5]

$$\mathbf{i} := \mathbf{jk} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

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

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

Είναι μάλιστα εύκολο να ελέγξει κανείς ότι αυτός *δεν* είναι μεταθετικός. Εξάλλου, θεωρώντας ένα στοιχείο του

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

ένα 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 $\neq 0$. Επομένως ο αντίστροφός του πίνακας

$$\frac{1}{a^2+b^2+c^2+d^2} \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix}$$

ορίζεται και ανήκει στο $\mathbb{H}_{\mathbb{R}}^{\times}$ (βλ. πρόταση 4.2.9). Άρα ο $\mathbb{H}_{\mathbb{R}}$ αποτελεί έναν *διαιρετικό δακτύλιο*[6], ο οποίος ονομάζεται **δακτύλιος των τετρανίων**[7] **υπεράνω τού σώματος** $\mathbb{R}$.

[5] Όπως προαναφέραμε στο προηγούμενο κεφάλαιο (βλ. 3.2.24 και 3.9.2), η λεγόμενη **ομάδα Q** $:= \langle \mathbf{j}, \mathbf{k} \rangle$ **των τετρανίων** υπεισέρχεται ουσιωδώς στην ταξινόμηση των πεπερασμένων ομάδων τάξεως 8.

[6] 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 $\mathbb{R}$.

[7] 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 στοιχειώδες σώμα $\mathbb{H}_{\mathbb{R}}$, πέραν τής συχνής χρήσεώς του στη Διανυσματική Ανάλυση, υπεισέρχεται και σε εφαρμογές τόσο τής σύγχρονης Αλγεβρικής Τοπολογίας όσο και τής Μαθηματικής Φυσικής.

4.2.15 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 $\mathrm{Zdv}(S) \subseteq \mathrm{Zdv}(R) = \varnothing$. □

4.2.16 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 πολλαπλασιαστικό στοιχείο.

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

4.2.18 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 $\mathbb{Z}^\times = \{-1, +1\} \subsetneqq \mathbb{Z}\smallsetminus\{0\}$, και ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. άσκ. ??), αφού

$$\mathrm{Zdv}(\mathbb{Z}[i]) = \varnothing \qquad \mathbb{Z}[i]^\times = \{-1, +1, -i, i\} \subsetneqq \mathbb{Z}[i]\smallsetminus\{0\}.$$

Από την άλλη μεριά, για *πεπερασμένους* μεταθετικούς 1-δακτυλίους με $1_R \neq 0_R$ οι έννοιες ακεραία περιοχή και σώμα ταυτίζονται (βλ. πρόταση 4.2.21).

4.2.19 Σημείωση. Εάν ο R είναι μια ακεραία περιοχή και ο S υποδακτύλιος τού R ο οποίος συμβαίνει να είναι ακεραία περιοχή ως προς τις ίδιες πράξεις, τότε ο S καλείται **υποπεριοχή** τής ακεραίας περιοχής R. 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 $\mathbb{Z} \subsetneqq R \subsetneqq \mathbb{Q}$ (βλ. άσκηση ??).

4.2.20 Σημείωση. Εάν το L είναι ένα σώμα και το K ένας υποδακτύλιος τού L ο οποίος συμβαίνει να είναι σώμα ως προς τις ίδιες πράξεις, τότε το K καλείται **υπόσωμα** τού L. Επί παραδείγματι, το $\mathbb{Q}$ είναι υπόσωμα τού $\mathbb{R}$ και το $\mathbb{R}$ υπόσωμα τού $\mathbb{C}$. Επίσης, για ακεραίους $m \in \mathbb{Z}\smallsetminus\{0, 1\}$, οι οποίοι δεν είναι τέλεια τετράγωνα, τα λεγόμενα **τετραγωνικά αριθμητικά σώματα** $\mathbb{Q}(\sqrt{m})$ (με τις αυτονόητες πράξεις προσθέσεως και πολλαπλασιασμού, βλ. άσκηση ??) αποτελούν υποσώματα τού σώματος $\mathbb{R}$ των πραγματικών αριθμών, όταν $m \in \mathbb{N},\ m \geq 2$, και υποσώματα τού σώματος $\mathbb{C}$ των μιγαδικών αριθμών, όταν $m \in \mathbb{Z},\ m \leq -1$.

4.2.21 Πρόταση. *Κάθε πεπερασμένος μη τετριμμένος* 1*-δακτύλιος ο οποίος δεν διαθέτει ούτε αριστερούς ούτε δεξιούς μηδενοδιαιρέτες είναι διαιρετικός. Και 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 κανόνα τής διαγραφής 4.2.5, για $c, c' \in R$ με $\beta(c) = \beta(c')$, παίρνουμε $c = c'$. Άρα η β, ως ενριπτική απεικόνιση, θα είναι και επιριπτική κατά το λήμμα 1.12.4. 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.) □

4.2.22 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.*

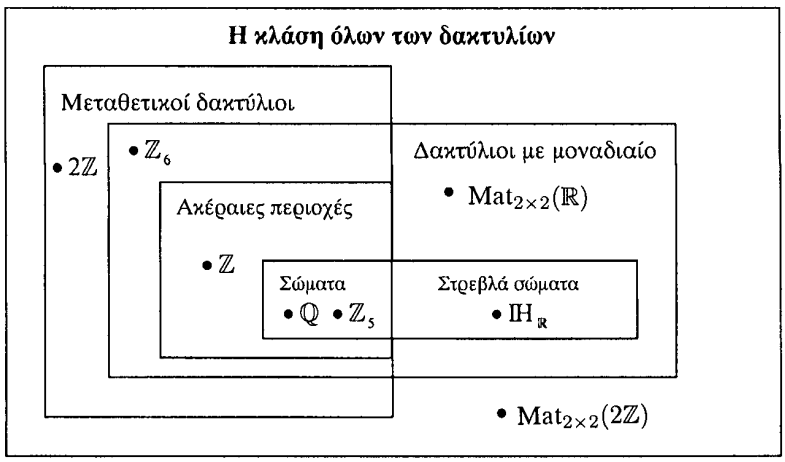
ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή (i) ⇒ (ii) έπεται από την πρόταση 4.2.4, η (ii) ⇒ (iii) από την πρόταση 4.2.21, και η (iii) ⇒ (ii) από την πρόταση 4.2.17. Τέλος, για τη συνεπαγωγή (ii) ⇒ (i) ας υποθέσουμε ότι ο m είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $m = pq$ δύο άλλων ακεραίων p, q, όπου $1 < p, q < m$. 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). □

4.2.23 Θεώρημα. (Wedderburn, 1905) *Κάθε πεπερασμένος διαιρετικός δακτύλιος είναι σώμα.*

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

4.2.24 Σύνοψη. 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:



4.3 Η ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΤΩΝ ΔΑΚΤΥΛΙΩΝ

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

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

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

4.3.2 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, $\text{χαρ}(R) = 1 \iff$ ο R είναι ο τετριμμένος δακτύλιος.

4.3.3 Πρόταση. *Έστω R ένας 1-δακτύλιος. Τότε*

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

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 $k = n$. □

4.3.4 Πρόταση. *Η χαρακτηριστική μιας 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

$$(k \cdot 1_R) = 0_R \;\; \text{ή} \;\; (l \cdot 1_R) = 0_R,$$

πράγμα που αντιφάσκει προς το γεγονός ότι ο n είναι ο *ελάχιστος* φυσικός αριθμός με αυτήν την ιδιότητα (βλ. πρόταση 4.3.3). Άρα τελικώς ο n οφείλει να είναι πρώτος αριθμός. □

4.3.5 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

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

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

(ii) Εάν χαρ$(R) = p$ (p πρώτος) και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$, τότε -από τον ορισμό τής χαρακτηριστικής- προκύπτει ότι

$$\text{ord}\,(a) \leq p.$$

Όμως η ισότητα $0_R = \text{ord}(a)\, a = (\text{ord}\,(a) \cdot 1_R)\, a$ μας δίνει 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 4.3.3. Συνεπώς, $\text{ord}(a) = p$. □

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

4.3.7 Πρόταση. *Εάν η 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) $(a+b)^p = a^p + b^p$.
(ii) $(a+b)^{p^r} = a^{p^r} + b^{p^r}$ *για κάθε* $r \in \mathbb{N}$.
(iii) $(a_1 + \cdots + a_n)^p = a_1^p + \cdots + a^p$.
(iv) $(a_1 + \cdots + a_n)^{p^r} = a_1^{p^r} + \cdots + a_n^{p^r}$ *για κάθε* $r \in \mathbb{N}$.

4.4 ΟΜΟΜΟΡΦΙΣΜΟΙ ΔΑΚΤΥΛΙΩΝ

4.4.1 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι και η

$$f : R \longrightarrow R'$$

μια απεικόνιση, τότε η f καλείται **ομομορφισμός** όταν ισχύουν οι ισότητες

$$\boxed{f\,(a+b) = f\,(a) + f\,(b)} \qquad \text{και} \qquad \boxed{f\,(ab) = f\,(a)\, f\,(b)} \tag{4.6}$$

για όλα τα $a, b \in R$.

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

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιριπτική,
ενδομορφισμός (**τού** R)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$R = R'$ (και με ταυτιζόμενες πράξεις),
αυτομορφισμός (**τού** R)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιριπτικός ενδομορφισμός τού R.

(Φυσικά, αυτές οι έννοιες εμπεριέχουν τις αντίστοιχες έννοιες για τις επί μέρους δομές, δηλαδή εκείνες των εκάστοτε μετεχουσών αβελιανών προσθετικών ομάδων και πολλαπλασιαστικών ημιομάδων).

4.4.2 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 4.3.7 (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 $m \in \mathbb{Z} \setminus \{0, 1\}$ ένας ακέραιος αριθμός, ο οποίος δεν είναι τέλειο τετράγωνο, και

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subsetneqq \mathbb{C}$$

το αριθμητικό τετραγωνικό σώμα το αντιστοιχιζόμενο στον m (βλ. 4.2.20 και την άσκηση **4-30**). 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 $\mathbb{Q}(\sqrt{m})$.

(vii) Η *μηδενική απεικόνιση* $f : R \longrightarrow S$ μεταξύ δακτυλίων R και S, όπου $f(a) = 0$ για κάθε $a \in R$, είναι ένας ομομορφισμός δακτυλίων (*μηδενικός ομομορφισμός*). Σημειωτέον ότι όταν κανείς εκ των R, S δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιριπτικός.

4.4.3 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. Η απόδειξη έπεται κατόπιν χρήσεως των τύπων (4.6) και μαθηματικής επαγωγής επί τού n. □

4.4.4 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

$$\begin{aligned} (g \circ f)(a+b) &= g(f(a+b)) = g(f(a) + f(b)) \\ &= g(f(a)) + g(f(b)) \\ &= (g \circ f)(a) + (g \circ f)(b) \end{aligned}$$

και

$$\begin{aligned} (g \circ f)(ab) &= g(f(ab)) = g(f(a)\, f(b)) \\ &= g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b), \end{aligned}$$

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), βλ. πρόταση 1.2.15 (i), (ii). □

4.4.5 Συμβολισμός. Εάν οι R και R' είναι δυο δακτύλιοι, τότε γράφουμε[8] $R \cong R'$ και λέμε ότι **ο** R **είναι ισόμορφος με τον** R' (ή, απλούστερα, ότι **ο** R **είναι ισόμορφος τού** R') όταν υπάρχει κάποιος ισομορφισμός $f : R \longrightarrow R'$.

4.4.6 Πρόταση. *Για οιουσδήποτε δακτυλίους R, R', R'' ισχύουν τα εξής*:

(i) $R \cong R$,

[8] Από τούδε και στο εξής μέσω τού συμβόλου "$\cong$" θα εκφράζουμε την ύπαρξη ισομορφισμών *δακτυλίων*. Ωστόσο, επειδή χρησιμοποιήσαμε το *ίδιο* σύμβολο *και* για τους ισομορφισμούς *ομάδων*, οφείλουμε να είμαστε ιδιαίτερα προσεκτικοί (πρβλ. 4.4.2 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.

(ii) $R \cong R' \Longrightarrow R' \cong R$,

(iii) $[R \cong R' \ \textit{και} \ R' \cong R''] \Longrightarrow R \cong R''$.

Ως εκ τούτου, η "$\cong$" ορίζει μια σχέση ισοδυναμίας επί τής «κλάσεως» των δακτυλίων.

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 4.4.4, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός δακτυλίων. □

4.4.7 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*:

$$f(na) = n\, f(a), \quad \forall n \in \mathbb{Z},$$

και

$$f(a^n) = f(a)^n, \quad \forall n \in \mathbb{N}.$$

(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 1-δακτύλιος, τότε και ο $f(R)$ είναι ένας 1-δακτύλιος με $f(1_R) = 1_{f(R)}$.*

(vi) *Εάν ο R είναι ένας 1-δακτύλιος, η f δεν είναι ο μηδενικός ομομορφισμός, και ο R' είναι ένας 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 οι R είναι ένας 1-δακτύλιος, τότε*

$$f(a^{-1}) = [f(a)]^{-1} \in f(R)^{\times}, \ \ \forall a, \ \ a \in R^{\times},$$

και, γενικότερα,

$$f(a^n) = f(a)^n, \ \ \forall a \in R^{\times} \text{ και } \forall n \in \mathbb{Z}.$$

(ix) *Εάν ο 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 4.4.3 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 $f(a) = b$. Άρα

$$f(1_R) f(a) = f(1_R a) = f(a), \qquad f(a) f(1_R) = f(a 1_R) = f(a),$$

οπότε ο $f(R)$ είναι ένας 1-δακτύλιος με $f(1_R) = 1_{f(R)}$.

(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

$$f(a) \cdot 1_{R'} = f(a) = f(a \cdot 1_R) = f(a) f(1_R) \Longrightarrow f(a)\,(f(1_R) - 1_{R'}) = 0_{R'}.$$

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 $f(1_R) = 1_{R'}$. Εάν, από την άλλη μεριά, ο R είναι ακεραία περιοχή, τότε μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα κάνοντας χρήση τού κανόνα τής διαγραφής 4.2.5.

(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 $f(1_R) = 1_{f(R)}$, έχουμε $f(a^{-1}) = [f(a)]^{-1} \in f(R)^\times$. 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 $a, b \in R$, ούτως ώστε να ισχύει

$$f(a)f(b) = 0_{f(R)} \Longleftrightarrow f(ab) = 0_{f(R)} = f(0_R),$$

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 $f(a^{-1}) = [f(a)]^{-1} \in f(R)^\times$ (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).) □

4.4.8 Πρόταση. *Εάν ο $f : K \longrightarrow R$ είναι ένας ομομορφισμός δακτυλίων, όπου ο K είναι ένας διαιρετικός δακτύλιος (= στρεβλό σώμα) και ο R ένας 1-δακτύλιος, τότε ο f είναι ή ο μηδενικός ομομορφισμός ή ένας μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Εάν ο f δεν είναι ο μηδενικός ομομορφισμός (ήτοι δεν ισχύει $f(a) = 0$, *για κάθε* $a \in K$) και εάν -επιπροσθέτως- υποθέσουμε ότι $f(x) = f(y)$ για κάποια $x, y \in K$, τότε

$$f(x - y) = f(x) - f(y) = 0_R. \tag{4.7}$$

Εάν $x-y \neq 0_K$, τότε το $x-y$ θα διαθέτει πολλαπλασιαστικό αντίστροφο $(x-y)^{-1}$. Αυτό, κατά την 4.4.7 (viii), σημαίνει ότι

$$f((x-y)^{-1}) = (f(x-y))^{-1}. \tag{4.8}$$

Από τις (4.7) και (4.8) συνάγουμε ότι $0_R = f(x-y)(f(x-y))^{-1} = 1_R$, πράγμα άτοπο. Επομένως, $x = y$, και ο f είναι κατ' ανάγκην μονομορφισμός. □

4.4.9 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 4.4.8. □

4.4.10 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.

4.4.11 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. □

4.4.12 Ορισμός. Λέμε ότι ο δακτύλιος R μπορεί να **εμφυτευθεί** σε έναν δακτύλιο R' όταν υπάρχει ένας μονομορφισμός δακτυλίων $f : R \longrightarrow R'$.

4.4.13 Πρόταση. *Κάθε δακτύλιος R μπορεί να εμφυτευθεί σε έναν 1-δακτύλιο R'. Μάλιστα ο R' μπορεί να επιλεγεί κατά τέτοιον τρόπο, ώστε $\chi\alpha\rho(R') = 0$ ή $\chi\alpha\rho(R') = \chi\alpha\rho(R)$.*

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 κάθε (m, a), $(n, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής 0 με μοναδιαίο του στοιχείο το $(1, 0)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto (0, a)\,,$$

είναι ένας μονομορφισμός. Εάν $\text{χαρ}(R) = k > 0$, 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 $([1]_k\,, 0)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto ([0]_k\,, a)\,,$$

είναι και πάλι ένας μονομορφισμός. □

4.4.14 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. 4.4.15). Ωστόσο, όπως θα δούμε σε στην ενότητα 4.7 (βλ. πρόταση 4.7.5), *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί κατά τρόπο φυσικό σε ένα σώμα.

4.4.15 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 ακολούθου μονομορφισμού:

$$\mathbb{C} \hookrightarrow \mathbb{H}_{\mathbb{R}}, \;\; a + bi \longmapsto a\mathbf{I} + b\mathbf{j} = \begin{pmatrix} a + bi & 0 \\ 0 & a - bi \end{pmatrix},$$

όπου οι $\mathbf{I}$ και $\mathbf{j}$ είναι οι πίνακες οι εισαχθέντες στο 4.2.14 (ii).

(ii) Εάν στην πρόταση 4.4.13 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 $n \in \mathbb{Z} \setminus \{0\}$ ισχύει η ισότητα:

$$(-2, 2)\,(, 0, 2n) = (0, 0 - 4n + 4n) = (0, 0).$$

4.5 ΙΔΕΩΔΗ

Ένα «ιδεώδες[9]» ενός δακτυλίου R είναι ένας ειδικής φύσεως υποδακτύλιος τού R, ο οποίος (όπως θα διαπιστώσουμε στην επομένη ενότητα) *συμπεριφέρεται ιδεωδώς* σε ό,τι αφορά στη δόμηση «πηλικοδακτυλίου», σε πλήρη αναλογία με ό,τι συμβαίνει με τις *ορθόθετες υποομάδες* μιας δεδομένης ομάδας. (Για τον αντίστοιχο σχηματισμό πηλικοομάδας, βλ. 3.6.20.)

4.5.1 Ορισμός. Έστω R ένας δακτύλιος. Ένας υποδακτύλιος I τού 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.

4.5.2 Πρόταση. *Ένα μη κενό υποσύνολο I ενός δακτυλίου 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 $(R, +, \cdot)$. □

4.5.3 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) Έστω R ένας δακτύλιος και $n, k \in \mathbb{N}, 1 \leq k \leq n$. Ορίζουμε τα

$$I_k := \{\mathbf{A} = (a_{ij}) \in \mathrm{Mat}_{n\times n}(R) \mid a_{ij} = 0 \text{ όταν } j \neq k\}$$

και

$$J_k := \{\mathbf{A} = (a_{ij}) \in \mathrm{Mat}_{n\times n}(R) \mid a_{ij} = 0 \text{ όταν } i \neq k\}.$$

[9] 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.

Τότε τα I_k αποτελούν αριστερά, αλλ' εν γένει μη δεξιά ιδεώδη, και τα J_k δεξιά, αλλ' εν γένει μη αριστερά ιδεώδη τού $\mathrm{Mat}_{n\times n}(R)$ (πρβλ. άσκηση ??).

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

(v) Εάν ο R είναι ένας δακτύλιος και $a \in R$, τότε το σύνολο $Ra := \{ra \mid r \in R\}$ είναι ένα αριστερό και το σύνολο $aR := \{ar \mid r \in R\}$ ένα δεξιό ιδεώδες τού R.

4.5.4 Παρατήρηση. Σε μεταθετικούς δακτυλίους δεν υφίσταται λόγος διακρίσεως μεταξύ δεξιών και αριστερών ιδεωδών.

4.5.5 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

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

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

4.5.6 Πρόταση. *Έστω R ένας 1-δακτύλιος. 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 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 ισούνται με 1_R) οφείλουν να ανήκουν στο I. Άρα

$$1_R \in I \Longrightarrow [\forall r \in R : r \cdot 1_R = r \in I] \Longrightarrow I = R,$$

πράγμα που έχουμε εκ των προτέρων αποκλείσει. □

4.5.7 Πόρισμα. *Έστω R ένας 1-δακτύλιος. Εάν το I είναι ένα γνήσιο (αριστερό/ δεξιό/ αμφίπλευρο) ιδεώδες τού R, τότε το I δεν περιέχει το 1_R.*

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

ΑΠΟΔΕΙΞΗ. Προφανής, αφού κάθε μη μηδενικό στοιχείο ενός διαιρετικού δακτυλίου είναι αντιστρέψιμο. □

4.5.9 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. □

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

4.5.10 Ορισμός. Έστω R ένας δακτύλιος και έστω A ένα υποσύνολο τού R. Τότε η τομή

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

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

4.5.11 Πρόταση. *Έστω R ένας δακτύλιος και έστω A ένα υποσύνολο τού R.*

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

$$\sum_{i=1}^{\kappa} r_i a_i s_i + \sum_{j=1}^{\mu} r'_j a'_j + \sum_{k=1}^{\nu} a''_k s''_k + \sum_{\varrho=1}^{\xi} n_\varrho a'''_\varrho \tag{4.9}$$

$$r_i, s_i, r'_j, s''_k \in R,\ \ a_i, a'_j, a''_k, a'''_\varrho \in A \ \ \textit{και}\ \ n_\varrho \in \mathbb{Z},$$
$$\forall i \in \{1, ..., \kappa\},\ \ \forall j \in \{1, ..., \mu\},\ \ \forall k \in \{1, ..., \nu\},\ \ \forall \varrho \in \{1, ..., \xi\},$$

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

(ii) *Εάν ο R είναι ένας* 1*-δακτύλιος, 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 ένας μεταθετικός δακτύλιος, τότε*

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

(iv) *Εάν ο R είναι ένας μεταθετικός* 1*-δακτύλιος, 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 (4.9). Τόσο η διαφορά δυο στοιχείων τής μορφής (4.9), όσο και το γινόμενο ενός $r \in R$ με οιοδήποτε στοιχείο τής μορφής (4.9), έχουν και πάλι τη μορφή (4.9). 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 (4.9), οπότε έχουμε $I \subseteq \langle A\rangle$.

(ii) Εάν ο R είναι ένας 1-δακτύλιος, τότε τα αθροίσματα τής μορφής (4.9) μπορούν να «συμπτυχθούν» (κατά τα αναγραφόμενα), αφού

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

και

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

(iii) Εάν ο R είναι ένας μεταθετικός δακτύλιος, τότε τα αθροίσματα τής μορφής (4.9) 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 1-δακτύλιος, τότε ενσωματώνουμε στο $\langle A\rangle$ και τα δύο είδη «συμπτύξεων» τής μορφής των στοιχείων που περιγράψαμε προηγουμένως στα (ii) και (iii). □

4.5.12 Σημείωση. Εάν ο R είναι ένας δακτύλιος και το A ένα υποσύνολο τού 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 4.5.11 για το $\langle A\rangle$.

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

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

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

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

(ii) *Εάν ο R είναι ένας* 1*-δακτύλιος, τότε*

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

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

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

(iv) *Εάν ο R είναι ένας μεταθετικός* 1*-δακτύλιος, τότε*

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

4.5.14 Παρατήρηση. Όταν ο R *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 $2 \notin (2\mathbb{Z})\, 2$.

4.5.15 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 $\{0\} \subsetneq I$, τότε υπάρχει κάποιος ακέραιος $n \in I\smallsetminus\{0\}$. Άρα και ο αντίθετός του ανήκει στο $I\smallsetminus\{0\}$ (αφού $-n = 0 - n$ με $0 \in I$ και $n \in I$). Ως εκ τούτου, *κάθε* μη τετριμμένο ιδεώδες I τού $\mathbb{Z}$ περιέχει *θετικούς ακεραίους*. Έστω

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

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

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

(βλ. θεώρημα 2.1.6), 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 $I = \langle n_0\rangle = \langle -n_0\rangle$. □

► **Δακτύλιοι με «λίγα» ιδεώδη**. Υπάρχουν δακτύλιοι με *μικρό αριθμό ιδεωδών*, οι οποίοι αξίζουν ιδιαίτερης μνείας.

4.5.16 Ορισμός. Ένας δακτύλιος ονομάζεται **απλός δακτύλιος** όταν δεν διαθέτει γνήσια (αμφίπλευρα) ιδεώδη[10].

4.5.17 Πρόταση. *Ένας μεταθετικός* 1*-δακτύλιος* R *είναι σώμα εάν και μόνον εάν είναι απλός.*

ΑΠΟΔΕΙΞΗ. Κάθε σώμα είναι ένας απλός μεταθετικός 1-δακτύλιος δυνάμει τού πορίσματος 4.5.8. Για την απόδειξη τού αντιστρόφου ισχυρισμού αρκεί να ελεγχθεί η ύπαρξη αντιστρόφου οιουδήποτε $x \in R\smallsetminus\{0\}$. Έστω $\langle x\rangle = Rx$ το κύριο ιδεώδες το παραγόμενο από το x. Το $\langle x\rangle$ δεν είναι τετριμμένο, καθότι $x = 1_R x \in \langle x\rangle$. Εξ υποθέσεως, ο R είναι απλός. Ως εκ τούτου, $\langle x\rangle = R$. Επειδή $1_R \in R = \langle x\rangle$, υπάρχει $r \in R$, τέτοιο ώστε $1_R = rx = xr$ (με την τελευταία ισότητα ισχύουσα λόγω τής μεταθετικότητας). Άρα $r = x^{-1}$. □

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

[10] Ο εν λόγω ορισμός είναι ανάλογος εκείνου των *απλών ομάδων* (βλ. άσκηση **3-34**).

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

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

οπότε υπάρχουν $j_0, k_0 \in \{1, ..., n\}$ με $a_{j_0k_0} \neq 0_R$. Έστω ότι ο $\mathbf{E}_{jk} \in \mathrm{Mat}_{n\times n}(R)$ είναι ο βοηθητικός πίνακας, ο οποίος έχει ως εγγραφή του στη θέση (j,k) το 1_R και σε όλες τις άλλες θέσεις εγγραφές που ισούνται με το 0_R. Τότε για κάθε δείκτη $p \in \{1, 2, ..., n\}$ λαμβάνουμε[11]

$$\mathbf{E}_{pj_0}\, \mathbf{A}\, \mathbf{E}_{k_0p} = a_{j_0k_0}\mathbf{E}_{pp}.$$

Επειδή $\mathbf{A} \in I$ και $\mathbf{E}_{pj_0}, \mathbf{E}_{k_0p} \in \mathrm{Mat}_{n\times n}(R)$, τούτο σημαίνει ότι $a_{j_0k_0}\mathbf{E}_{pp} \in I$. Επιπροσθέτως, επειδή ο R είναι διαιρετικός δακτύλιος, ορίζεται το αντίστροφο στοιχείο $a_{j_0k_0}^{-1}$ τού $a_{j_0k_0}$. Ως εκ τούτου,

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

απ' όπου έπεται ότι

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

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

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

ΑΠΟΔΕΙΞΗ. Έστω $a \in R\setminus\{0\}$. 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 ακόλουθη «κατιούσα» αλυσίδα διαδοχικώς εγκλειομένων κυρίων ιδεωδών:

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

[11] Ο πίνακας $a_{j_0k_0}\mathbf{E}_{pp}$ δηλοί *αριθμητικό πολλαπλασιασμό* τού $\mathbf{E}_{pp}$ με τον $a_{j_0k_0}$ και είναι -ως εκ τούτου- ο πίνακας που έχει ως εγγραφή του στη θέση (j_0, k_0) το $a_{j_0k_0}$ και σε όλες τις άλλες θέσεις εγγραφές που ισούνται με το 0_R.

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

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

Όμως τούτο έχει ως συνέπεια το ότι $a^n(1_R - ra) = 0_R$, το οποίο, συνδυαζόμενο με τον κανόνα τής διαγραφής, μας δίνει $ra = 1_R$, οπότε το r είναι (πολλαπλασιαστικό) αντίστροφο τού (αυθαιρέτως επιλεγμένου) μη μηδενικού στοιχείου a. □

► **Πράξεις οριζόμενες επί των ιδεωδών**. 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.

4.5.20 Ορισμός. Έστω ότι ο R είναι ένας δακτύλιος και τα $I_1, \ldots, I_n$ αριστερά (και αντιστοίχως, δεξιά/αμφίπλευρα) ιδεώδη του. Ορίζουμε το **άθροισμα** και το **γινόμενό** τους ως:

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

και

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

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

4.5.21 Σημείωση. (i) Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός 1-δακτυλίου R, τότε

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

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

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

κάθε $x \in \langle I_1 \cup \cdots \cup I_n \rangle$ μπορεί (ενδεχομένως ύστερα από κάποια αναδιάταξη δεικτών) να γραφεί υπό τη μορφή

$$x = x_1 + x_2 + \cdots + x_n,$$

όπου για κάθε $j \in \{1, \ldots, n\}$,

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

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

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

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

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

Επί παραδείγματι, εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων (πρβλ. 4.5.26 (iii)), έχουμε

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

Οι προτάσεις 4.5.22, 4.5.23, 4.5.24 και 4.5.27, οι οποίες ακολουθούν, έχουν ως στόχο την περιγραφή ορισμένων βασικών αρχών τού «λογισμού με ιδεώδη».

4.5.22 Πρόταση. *Εάν ο R είναι ένας μεταθετικός 1-δακτύλιος 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 την 4.5.21 (i).

(ii) Προφανώς,

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

όπου $Rab = \langle ab\rangle$. □

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

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

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

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

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

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

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

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

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

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

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

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

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

Επομένως, λόγω τής επιμεριστικής ιδιότητας,

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας,

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

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

4.5.24 Πρόταση. *Έστω ότι ο R είναι ένας δακτύλιος και τα I_1, I_2, I_3 ιδεώδη του. Τότε ισχύουν τα εξής*:
(i) $I_1 \, I_2 \subseteq I_1 \cap I_2$.
(ii) $(I_1 + I_2) \ (I_1 + I_3) \subseteq I_1 + I_2 \, I_3 \subseteq I_1 + (I_2 \cap I_3)$.

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

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

Όμως, από τον ορισμό τού ιδεώδους,

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

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

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

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

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

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

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

και αποτελεί ένα ιδεώδες τού R.

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

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

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

κι επειδή $\text{μκδ}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, το πόρισμα 2.2.9 μας πληροφορεί ότι

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

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

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

ήτοι $\langle m\rangle \cap \langle n\rangle \subseteq \langle \text{εκπ}(m,n)\rangle$. Και αντιστρόφως· εάν $a \in \langle \text{εκπ}(m,n)\rangle$, τότε έχουμε $a = \mu\,\text{εκπ}(m,n)$, για κάποιον $\mu \in \mathbb{Z}$, οπότε, εφαρμόζοντας τον τύπο (2.13), λαμβάνουμε

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

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

(ii) Κατά την πρόταση 4.5.22 (i), $\langle m\rangle + \langle n\rangle = \{\,xm + yn \mid x, y \in \mathbb{Z}\}$. Επειδή ο μέγιστος κοινός διαιρέτης των m και n γράφεται ως ακέραιος γραμμικός συνδυασμός των m και n (βλ. θεώρημα 2.2.5), έχουμε

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

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

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

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

(iii) Προφανές επί τη βάσει τής προτάσεως 4.5.22 (ii).

(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,

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

Εάν $d := \text{μκδ}(m,n)$, τότε $\text{μκδ}\big(\frac{m}{d}, \frac{n}{d}\big) = 1$, οπότε, κατά το πόρισμα 2.2.9,

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

για κάποιον $c \in \mathbb{Z}$. Άρα

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

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

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

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

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

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

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

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

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

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

οπότε

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

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

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

οπότε

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

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

(iv) Έστω τυχόν $r \in (I_1 : I_2) : I_3$. Τότε $ra \in I_1 : I_2,\ \forall a \in I_3$, οπότε

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

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

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

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

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

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

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

οπότε όντως $J_1 = J_2$. □

4.6 ΠΗΛΙΚΟΔΑΚΤΥΛΙΟΙ ΚΑΙ ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

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

$$(a + I) + (b + I) := (a + b) + I\,, \ \text{για κάθε} \ \ a, b \in R. \tag{4.10}$$

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

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

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

$$(a + I)\ (b + I) := (ab) + I\,. \tag{4.11}$$

Ας σημειωθεί ότι εάν ο R είναι μεταθετικός (και αντιστοίχως, 1*-δακτύλιος), τότε και ο R/I είναι μεταθετικός* (*και αντιστοίχως,* 1*-δακτύλιος με μοναδιαίο του στοιχείο το $1_R + I$*).

ΑΠΟΔΕΙΞΗ. Η πράξη τού «πολλαπλασιασμού» (4.11) είναι καλώς ορισμένη. Πράγματι· εάν υποθέσουμε ότι

$$a + I = a' + I, \quad b + I = b' + I,$$

για κάποια $a, a', b, b' \in R$, τότε $a' = a + r$ και $b' = b + s$, για κάποια $r, s \in I$. Επομένως,

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

απ' όπου συνάγουμε ότι $ab + I = a'b' + I$. Επίσης, η εν λόγω πράξη (4.11) είναι προφανώς μεταθετική όταν ο R είναι μεταθετικός, ενώ, όταν ο R είναι δακτύλιος με το 1_R ως μοναδιαίο στοιχείο, ο R/I είναι διαθέτει ως μοναδιαίο στοιχείο του το $1_R + I$. □

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

Η επομένη πρόταση δηλοί -κατ' ουσίαν- ότι οι έννοιες «πυρήνας ομομορφισμού δακτυλίων» και «ιδεώδες» μπορούν να χρησιμοποιούνται, η μία αντί τής άλλης, χωρίς περαιτέρω περιορισμούς.

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

ΑΠΟΔΕΙΞΗ. Ο πρώτος ισχυρισμός αποτελεί άμεση συνέπεια τής προτάσεως 4.5.9. Αλλά και αντιστρόφως: η απεικόνιση

$$\pi : R \longrightarrow R/I, \;\; \pi(r) := r + I, \; \forall r \in R,$$

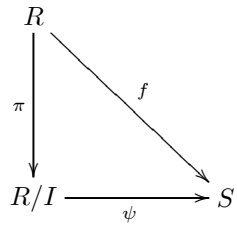
είναι ομομορφισμός δακτυλίων (λόγω των (4.10), (4.11)), εξ ορισμού επιρριπτική, και έχει ως πυρήνα της τον $\mathrm{Ker}(\pi) = \{ r \in R \mid r + I = I \} = I$. □

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

4.6.5 Θεώρημα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων, το I ένα ιδεώδες τού R, τέτοιο ώστε $I \subseteq \mathrm{Ker}(f)$, και $\pi : R \longrightarrow R/I$ ο φυσικός επιμορφισμός. Τότε η απεικόνιση*

$$\psi : R/I \longrightarrow S, \;\; (a + I) \longmapsto f(a), \; \forall a \in R,$$

είναι καλώς ορισμένη και αποτελεί έναν ομομορφισμό δακτυλίων, τέτοιον ώστε να έχουμε $\psi \circ \pi = f$.



Η απεικόνιση ψ *είναι επιρριπτική εάν και μόνον εάν η* f *είναι επιρριπτική, ενώ είναι ενριπτική εάν και μόνον εάν ισχύει η ισότητα* $I = \text{Ker}(f)$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς η ψ είναι καλώς ορισμένη (ως απεικόνιση), διότι εάν έχουμε $a + I = b + I$, για κάποια $a, b \in R$, τότε

$$a - b \in I \subseteq \text{Ker}\,(f) \Longrightarrow f(a-b) = f(a) - f(b) = 0_{R'} \Longrightarrow f(a) = f(b).$$

Επίσης, $\psi \circ \pi = f$, καθότι ισχύει

$$\psi\,(\pi\,(a)) = \psi\,(a + I) = f\,(a)\,,\ \ \forall a \in R.$$

Το ότι η ψ είναι και ομομορφισμός δακτυλίων συνάγεται από τις ακόλουθες ισότητες:

$$\begin{cases} \psi\,((a+I)+(b+I)) = \psi\,((a+b)+I) = f(a+b) \\ = f(a) + f(b) = \psi\,(a+I) + \psi\,(b+I)\,, \\ \psi\,((a+I)\,(b+I)) = \psi\,(ab+I) = f(ab) \\ = f(a)f(b) = \psi\,(a+I)\,\psi\,(b+I)\,,\ \forall a, b \in R. \end{cases}$$

Εξάλλου, επειδή η π είναι επιρριπτική, η $f = \psi \circ \pi$ είναι επιρριπτική εάν και μόνον εάν η ψ είναι επιρριπτική. Αρκεί λοιπόν να αποδειχθεί και η διπλή συνεπαγωγή:

$$(\psi \text{ ενριπτική}) \iff \text{Ker}\,(f) = I.$$

($\Longrightarrow$) Έστω τυχόν $a \in \text{Ker}(f)$. Τότε

$$\psi\,(a+I) = f(a) = 0_S = \psi\left(0_{R/I}\right) = \psi\,(I) \underset{[\psi \text{ ένριψη}]}{\Longrightarrow} a + I = I \Longrightarrow a \in I.$$

Άρα $\text{Ker}(f) \subseteq I$. Κι επειδή -εξ υποθέσεως- $I \subseteq \text{Ker}(f)$, έχουμε $\text{Ker}(f) = I$.

($\Longleftarrow$) Εάν υποθέσουμε ότι $\text{Ker}(f) = I$, αρκεί να δείξουμε (επί τη βάσει τής προτάσεως 4.4.11) ότι $\text{Ker}(\psi) = \{0_{R/I}\}$. Έστω λοιπόν τυχόν $a + I \in \text{Ker}(\psi)$. Τότε

$$f(a) = \psi\,(a+I) = 0_S \Longrightarrow a \in \text{Ker}\,(f) = I \Longrightarrow a + I = I = 0_{R/I},$$

απ' όπου έπεται ότι πράγματι $\text{Ker}(\psi) = \{0_{R/I}\}$. □

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

$$\boxed{R/\text{Ker}(f) \cong \text{Im}\,(f) = f\,(R)}$$

Μάλιστα, ένας συγκεκριμένος ισομορφισμός $\psi : R/\text{Ker}(f) \xrightarrow{\cong} \text{Im}(f)$ καθορίζεται μέσω τής $\psi\,(a + \text{Ker}(f)) = f\,(a)$.

ΑΠΟΔΕΙΞΗ. Άμεση δυνάμει τού θεωρήματος 4.6.5, όταν θέσουμε $I = \text{Ker}(f)$. □

4.6.7 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, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Εξάλλου, επειδή $m\mathbb{Z} = -m\mathbb{Z}$ για κάθε $m \in \mathbb{Z}\setminus\{0\}$, έχουμε γενικότερα

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|},\ \forall m \in \mathbb{Z}\setminus\{0\}.} \tag{4.12}$$

(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,

$$\boxed{R/I \cong \mathbb{R}}$$

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:

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

Η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{Z}_2,\ \ \tfrac{a}{b} \longmapsto f(\tfrac{a}{b}) := \begin{cases} [0]_2\,, & \text{όταν } a \equiv 0 (\mathrm{mod}\, 2), \\ [1]_2\,, & \text{όταν } a \equiv 1 (\mathrm{mod}\, 2), \end{cases}$$

είναι ομομορφισμός δακτυλίων (γιατί;) και βάσει τού 1ου θεωρήματος ισομορφισμών

$$\boxed{R/\left\{ \tfrac{a}{b} \in R \,\middle|\, a \equiv 0 (\mathrm{mod}\, 2) \right\} \cong \mathbb{Z}_2.}$$

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

(i) *το $S \cap I$ είναι ένα μη τετριμμένο, γνήσιο 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 μη τετριμμένο, γνήσιο ιδεώδες τού $S + I$, και*

(iv) *έχουμε*

$$\boxed{S/(S \cap I) \cong (S + I)/I}$$

ΑΠΟΔΕΙΞΗ. (i) Επειδή το I είναι ένα μη τετριμμένο, γνήσιο ιδεώδες τού R, έχουμε

$$\{0_S\} = \{0_R\} \subsetneqq S \cap I \subsetneqq S.$$

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 μη τετριμμένο, γνήσιο 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) Επειδή το I είναι ένα μη τετριμμένο, γνήσιο ιδεώδες τού R, έχουμε

$$\{0_{S+I}\} = \{0_R\} \subsetneqq I \subsetneqq S + I.$$

Αρκεί λοιπόν να δειχθεί ότι το I είναι ένα ιδεώδες τού $S + I$. 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, $f = \pi \circ j$, όπου $\pi : S + I \longrightarrow (S + I)/I$ ο επιμορφισμός κλάσεων υπολοίπων και $j : S \longrightarrow S + I$ η συνήθης ένθεση $s \longmapsto s(+0_R)$. Κατά το 1ο θεώρημα ισομορφισμών 4.6.6, $S/\mathrm{Ker}(f) \cong f(S)$. 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. □

4.6.9 Πόρισμα. *Έστω ότι ο R είναι ένας δακτύλιος και I, J δύο ιδεώδη του. Τότε ισχύουν οι 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 4.6.8. Για την απόδειξη των δύο άλλων 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 ομομορφισμό 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 δακτυλίων 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 σε αμφότερους τους παράγοντες τού μετέχοντος καρτεσιανού γινομένου δακτυλίων. □

4.6.10 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle m \rangle$, $J = \langle n \rangle$, για κάποιους $m, n \in \mathbb{Z} \setminus \{0\}$, τότε, λαμβάνοντας υπ' όψιν τα όσα αποδείξαμε στα 4.5.26 (i), (ii), οι ισομορφισμοί οι θεσπισθέντες μέσω τού πορίσματος 4.6.9 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,

$$\begin{aligned} \langle \text{μκδ}(m,n) \rangle \,/\, \langle \text{εκπ}(m,n) \rangle &\cong (\langle \text{μκδ}(m,n) \rangle \,/\, \langle m \rangle) \times (\langle \text{μκδ}(m,n) \rangle \,/\, \langle n \rangle) \\ &\cong (\langle n \rangle \,/\, \langle \text{εκπ}(m,n) \rangle) \times (\langle m \rangle \,/\, \langle \text{εκπ}(m,n) \rangle)\,. \end{aligned}$$

4.6.11 Πόρισμα. *Εάν τα I, J είναι δυο ιδεώδη ενός δακτυλίου R και ισχύει*[12] *η ισότητα $R = I + J$, τότε*

$$\boxed{R/\,(I \cap J) \cong (R/I) \times (R/J)}$$

4.6.12 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 $f = \pi_2 \circ \pi_1$, όπου $\pi_1 : R \longrightarrow (R/I)$ και $\pi_2 : R/I \longrightarrow (R/I) \,/\, (J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας (καλώς ορισμένος) επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 4.6.6,

$$R/\mathrm{Ker}\,(f) \cong (R/I) \,/\, (J/I)\,.$$

[12] Δυο ιδεώδη I, J, τα οποία πληρούν αυτήν τη συνθήκη, λέγονται ιδιαιτέρως **συμμεγιστοτικά**.

Όμως

$$\begin{aligned}\mathrm{Ker}(f) &= \left\{ a \in R \mid f(a) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \left\{ a \in R \mid \pi_2(\pi_1(a)) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \left\{ a \in R \mid \pi_2(a+I) = 0_{(R/I)\,/\,(J/I)} \right\} \\ &= \{ a \in R \mid a + I \in \mathrm{Ker}\,(\pi_2) \} \\ &= \{ a \in R \mid a + I \in (J/I) \} = J,\end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

4.6.13 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 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. 4.6.6 και 4.6.12),

$$\mathbb{Z}_3 = \{[0]_3\,, [1]_3\,, [2]_3\} \cong \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/I)\ /\,(J/I) = \{(J/I, 1 + (J/I), 2 + (J/I)\}.$$

4.7 ΣΩΜΑΤΑ ΚΛΑΣΜΑΤΩΝ ΑΚΕΡΑΙΩΝ ΠΕΡΙΟΧΩΝ

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 μεθόδου κατασκευής των ρητών αριθμών από τους ακεραίους.

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

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

Έστω

$$\boxed{\mathbf{Fr}(R):=(R\times(R\smallsetminus\{0\}))\,/\sim}$$

το σύνολο κλάσεων ισοδυναμίας ως προς την "$\sim$". Το **κλάσμα** ενός $a\in R$ «διηρημένου» διά ένα $b\in R\smallsetminus\{0\}$ είναι η κλάση ισοδυναμίας

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

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

$$\begin{cases}\dfrac{a}{b}+\dfrac{c}{d} &:= \dfrac{ad+cb}{bd},\\[2ex] \dfrac{a}{b}\cdot\dfrac{c}{d} &:= \dfrac{ac}{bd}.\end{cases}$$

4.7.2 Πρόταση. *Οι εν λόγω πράξεις είναι καλώς ορισμένες.*

ΑΠΟΔΕΙΞΗ. Εάν για κάποια ζεύγη $(a,b)\,,(a',b')$ και $(c,d)\,,(c',d')\in R\times(R\smallsetminus\{0\})$ έχουμε

$$[(a,b)]=[(a',b')]\quad\text{και}\quad[(c,d)]=[(c',d')]\,,$$

τότε

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}\ \text{ και }\ \frac{a}{b}\frac{c}{d}=\frac{a'}{b'}\frac{c'}{d'}.$$

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 $\frac{a}{b}\frac{c}{d} = \frac{a'}{b'}\frac{c'}{d'}$. □

4.7.3 Πρόταση. *Το σύνολο* $\mathbf{Fr}(R)$ *όλων 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*** *τής* R*.)*

ΑΠΟΔΕΙΞΗ. Η μεταθετικότητα και προσεταιριστικότητα τής προσθέσεως ελέγχονται εύκολα, καθότι

$$\tfrac{a}{b} + \tfrac{c}{d} = \tfrac{ad+cb}{bd} = \tfrac{cb+ad}{bd} = \tfrac{c}{d} + \tfrac{a}{b}$$

και

$$\begin{aligned}\left(\tfrac{a}{b} + \tfrac{c}{d}\right) + \tfrac{e}{f} &= \tfrac{ad+cb}{bd} + \tfrac{e}{f} = \tfrac{adf+cbf+ebd}{bdf} \\ &= \tfrac{adf+(cf+ed)b}{bdf} = \tfrac{a}{b} + \tfrac{cf+ed}{df} = \tfrac{a}{b} + \left(\tfrac{c}{d} + \tfrac{e}{f}\right)\end{aligned}$$

για οιαδήποτε $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$. Παρομοίως ελέγχεται η μεταθετικότητα και η προσεταιριστικότητα τού πολλαπλασιασμού, καθώς και οι επιμεριστικότητα ως προς τις ορισθείσες πράξεις. Το μηδενικό στοιχείο τού $\mathbf{Fr}(R)$ είναι το $\frac{0}{1}$, το αντίθετο τού $\frac{a}{b}$ το $\frac{-a}{b}$, το μοναδιαίο στοιχείο το $\frac{1}{1}$ και, τέλος, το αντίστροφο καθενός $\frac{a}{b} \in \mathbf{Fr}(R) \setminus \{\frac{0}{1}\}$ το $\frac{b}{a}$. □

4.7.4 Παράδειγμα. Προφανώς, $\mathbf{Fr}(\mathbb{Z}) = \mathbb{Q}$.

4.7.5 Πρόταση. *Κάθε ακεραία περιοχή εμφυτεύεται εντός τού σώματος των κλασμάτων της.*

ΑΠΟΔΕΙΞΗ. Εάν ο δακτύλιος R είναι ακεραία περιοχή, τότε ο ομομορφισμός

$$R \longrightarrow \mathbf{Fr}(R), \quad a \longmapsto \frac{a}{1},$$

είναι ένας μονομορφισμός, διότι έχει το $\{\, a \in R \mid \frac{a}{1} = \frac{0}{1}\} = \{0\}$ ως πυρήνα του (βλ. πρόταση 4.4.11). □

4.7.6 Πρόταση. *Εάν η* R *είναι μια ακεραία περιοχή και το* K *ένα σώμα το οποίο την περιέχει, τότε η απεικόνιση*

$$\psi : \mathbf{Fr}(R) \longrightarrow K,$$

η οριζόμενη μέσω των

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

αποτελεί μονομορφισμό σωμάτων.

ΑΠΟΔΕΙΞΗ. Η ψ είναι *ομομορφισμός*, καθότι για οιαδήποτε $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned}
\psi(\tfrac{a}{b}+\tfrac{c}{d}) &= \psi(\tfrac{ad+cb}{bd}) = \psi(ad+cb)\,\psi(bd)^{-1} = (ad+cb)\,(bd)^{-1} \\
&= (ad+cb)\,d^{-1}b^{-1} = (ad)\left(d^{-1}b^{-1}\right) + (cb)\left(d^{-1}b^{-1}\right) \\
&= a\left(dd^{-1}\right)b^{-1} + c\left(bb^{-1}\right)d^{-1} = ab^{-1} + cd^{-1} \\
&= \psi(a)\psi\left(b^{-1}\right) + \psi(c)\,\psi\left(d^{-1}\right) = \psi(\tfrac{a}{b}) + \psi(\tfrac{c}{d})
\end{aligned}$$

και

$$\begin{aligned}
\psi(\tfrac{a}{b}\,\tfrac{c}{d}) &= \psi(\tfrac{ac}{bd}) = \psi(ac)\,\psi(bd)^{-1} = (ac)\,(bd)^{-1} \\
&= (ab^{-1})(cd^{-1}) = \left(\psi(a)\psi\left(b^{-1}\right)\right)\left(\psi(c)\,\psi\left(d^{-1}\right)\right) \\
&= \psi(\tfrac{a}{b})\psi(\tfrac{c}{d}),
\end{aligned}$$

λόγω τής προσεταιριστικής και μεταθετικής ιδιότητας του πολλαπλασιασμού που ισχύουν για τα στοιχεία τού $K\smallsetminus\{0\}$ και τού ότι $\psi|_R := \mathrm{Id}_R$. Επιπροσθέτως, η ψ είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ με $\psi(\frac{a}{b}) = \psi(\frac{c}{d})$, τότε

$$\psi(a)\,\psi(b)^{-1} = \psi(c)\,\psi(d)^{-1} \Longrightarrow \psi(a)\,\psi(d) = \psi(b)\,\psi(c),$$

ήτοι

$$\psi(ad) = \psi(bc) \underset{[\,\psi|_R := \mathrm{Id}_R]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

απ' όπου έπεται ότι η ψ είναι πράγματι ένας *μονομορφισμός*. □

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

ΑΠΟΔΕΙΞΗ. Έστω K ένα άλλο σώμα που περιέχει την R. Για κάθε (a,b) που ανήκει στο $R\times(R\smallsetminus\{0\})$ έχουμε $ab^{-1} \in K$, διότι το K είναι σώμα και $R \subseteq K$. Ταυτίζοντας (μέχρις ισομορφισμού) την $\mathbf{Fr}(R)$ με την $\psi\,(\mathbf{Fr}(R))$ στην προηγηθείσα πρόταση, το $\frac{a}{b}$ ταυτίζεται με το ab^{-1}, οπότε ισχύει $\mathbf{Fr}(R) \cong \psi\,(\mathbf{Fr}(R)) \subseteq K$. □

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

ΑΠΟΔΕΙΞΗ. Εάν η απεικόνιση $f : R_1 \longrightarrow R_2$ είναι ένας ισομορφισμός, τότε και η απεικόνιση

$$\widetilde{f} : \mathbf{Fr}(R_1) \longrightarrow \mathbf{Fr}(R_2), \quad \widetilde{f}\left(\frac{a}{b}\right) := \frac{f(a)}{f(b)}, \ \forall\, (a,b) \in R_1 \times (R_1 \setminus \{0\}),$$

είναι ισομορφισμός. Πράγματι η $\widetilde{f}$ είναι *ομομορφισμός* σωμάτων, διότι για κάθε $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ έχουμε

$$\widetilde{f}(\tfrac{a}{b} + \tfrac{c}{d}) = \widetilde{f}(\tfrac{ad+cb}{bd}) = \tfrac{f(ad+cb)}{f(bd)} = \tfrac{f(ad)+f(cb)}{f(b)f(d)} = \tfrac{f(a)f(d)+f(c)f(b)}{f(b)f(d)} = \tfrac{f(a)}{f(b)} + \tfrac{f(c)}{f(d)}$$

και

$$\widetilde{f}(\tfrac{a}{b}\,\tfrac{c}{d}) = \widetilde{f}(\tfrac{ac}{bd}) = \tfrac{f(ac)}{f(bd)} = \tfrac{f(a)f(c)}{f(b)f(d)} = \tfrac{f(a)}{f(b)}\,\tfrac{f(c)}{f(d)} = \widetilde{f}(\tfrac{a}{b})\widetilde{f}(\tfrac{c}{d}).$$

Επιπροσθέτως, η $\widetilde{f}$ είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ με $\widetilde{f}(\frac{a}{b}) = \widetilde{f}(\frac{c}{d})$, τότε $\frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$, απ' όπου έπεται ότι

$$f(a)f(d) = f(c)f(b) \Longrightarrow f(ad) = f(cb) \underset{[f \text{ ένριψη}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

Τέλος, η $\widetilde{f}$ είναι και *επιριπτική* απεικόνιση, διότι για κάθε $\frac{c}{d} \in \mathbf{Fr}(R_2)$ υπάρχει ζεύγος $(a,b) \in R_1 \times (R_1 \setminus \{0\})$, τέτοιο ώστε να ισχύει

$$[f(a) = c, \quad f(b) = d] \Longrightarrow \widetilde{f}(\tfrac{a}{b}) = \tfrac{f(a)}{f(b)},$$

ήτοι $\widetilde{f}(\frac{a}{b}) = \frac{c}{d}$. □

4.8 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 4.7.7, 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».

4.8.1 Ορισμός. Ένα σώμα K καλείται **πρώτο σώμα** όταν δεν περιέχει κανένα γνήσιο υπόσωμα.

4.8.2 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 3.5.18 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 $L=\mathbb{Z}_p$.

4.8.3 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 υπάρξεως 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 $K_0=K_0'$. □

4.8.4 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,

$$\mathbb{Z}/\mathrm{Ker}\,(f)\cong \mathrm{Im}\,(f)=f(\mathbb{Z}),$$

όπου

$$\mathrm{Ker}\,(f)=\{\,n\in\mathbb{Z}\mid n\cdot 1_L=0_L\}.$$

(i) Εάν το L έχει χαρακτηριστική μηδέν, τότε $\mathrm{Ker}(f) = \{0\}$, οπότε

$$\mathbb{Z}/\mathrm{Ker}\,(f) = \mathbb{Z}/\{0\} \cong \mathbb{Z} \cong \mathrm{Im}\,(f) = f(\mathbb{Z}).$$

Ως εκ τούτου, η $\mathrm{Im}\,(f)$ είναι μια ακεραία περιοχή (ισόμορφη τής $\mathbb{Z}$) και, επειδή $\mathrm{Im}\,(f) \subseteq L$, έχουμε

$$\mathbf{Fr}\,(\mathrm{Im}\,(f)) = \left\{ \frac{n \cdot 1_L}{m \cdot 1_L} \;\middle|\; (n,m) \in \mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\}) \right\} \subseteq \mathbf{Fr}\,(L) = L,$$

οπότε $L = \mathbf{Fr}\,(\mathrm{Im}\,(f)) \cong \mathbf{Fr}\,(\mathbb{Z}) = \mathbb{Q}$ (λόγω τής προτάσεως 4.7.8 και τού ότι το L είναι πρώτο σώμα).

(ii) Εάν το L έχει χαρακτηριστική p, όπου p πρώτος αριθμός, τότε, βάσει τής προτάσεως 4.3.3 έχουμε

$$p = \min\{\,|k| \in \mathbb{N} \mid\; k \in \mathbb{Z}\smallsetminus\{0\} \;\text{ με }\; k \cdot 1_L = 0_L\},$$

οπότε $p \in \mathrm{Ker}(f) \Longrightarrow p\mathbb{Z} = \langle p\rangle \subseteq \mathrm{Ker}(f)$. Αλλά και για κάθε $\lambda \in \mathrm{Ker}(f)$, γράφοντας

$$\lambda = up + r, \;\; u, r \in \mathbb{Z}, \quad 0 \le r \le p-1,$$

(κατά το 2.1.6) 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 $\mathrm{Ker}(f) \subseteq p\mathbb{Z} = \langle p\rangle$. Τελικώς λοιπόν $\mathrm{Ker}(f) = p\mathbb{Z} = \langle p\rangle$ και

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p \cong \mathrm{Im}\,(f) = f(\mathbb{Z}) = \{\,n \cdot 1_L \mid\; n \in \{0, 1, \ldots, p-1\}\} \subseteq L,$$

απ' όπου συμπεραίνουμε ότι $L = \mathrm{Im}\,(f) \cong \mathbb{Z}_p$, διότι το L είναι πρώτο σώμα. □

4.8.5 Πόρισμα. *Κάθε σώμα K περιέχει ένα υπόσωμα L, τέτοιο ώστε*:

$$L \cong \begin{cases} \mathbb{Q}, & \text{όταν } \mathrm{χαρ}(K) = 0, \\ \\ \mathbb{Z}_p, & \text{όταν } \mathrm{χαρ}(K) = p > 0. \end{cases}$$

4.8.6 Παρατήρηση. Σύμφωνα με όσα αναφέραμε στην απόδειξη τού θεωρήματος 4.8.4, εάν το L είναι ένα πρώτο σώμα, τότε

$$L = \begin{cases} \left\{ (n \cdot 1_L)\,(m \cdot 1_L)^{-1} \;\middle|\; (n,m) \in \mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\}) \right\}, & \text{όταν } \mathrm{χαρ}(L) = 0, \\ \\ \{\,n \cdot 1_L \mid\; n \in \{0, 1, \ldots, p-1\}\}, & \text{όταν } \mathrm{χαρ}(L) = p > 0. \end{cases}$$