ΚΕΦΑΛΑΙΟ 1

Δακτύλιοι, ακέραιες περιοχές και σώματα

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

1.1 ΔΑΚΤΥΛΙΟΙ ΚΑΙ ΥΠΟΔΑΚΤΥΛΙΟΙ

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

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

[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).

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

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

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

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

1.1.2 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 ορισμό1.1.1 χωρίς όμως και να τη σημειώνουμε. Επίσης, εάν $n\in\mathbb{N}$ και εάν τα $a_1,\ldots,a_n$ είναι στοιχεία ενός δακτυλίου R, τότε χρησιμοποιούμε ενίοτε τις βραχυγραφίες

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

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

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

(ii) 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 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 $\mathrm{Mat}_{n\times n}(R)$, όπου R κάποιος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, παροτρύνουμε τον αναγνώστη, στο σημείο αυτό, να επιλύσει την άσκηση **1-13**).

(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 όλων των κλάσεων υπολοίπων κατά μόδιο m

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

αποτελεί έναν μεταθετικό δακτύλιο (με το $[1]_m$ ως μοναδιαίο στοιχείο[3]) βάσει των συνήθων πράξεων

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

για όλα τα $a, b \in \{0, 1, \ldots, m-1\}$.

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

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

Ιδιαιτέρως, εάν $X = \{1, \ldots, n\} \subset \mathbb{N}$, 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 αποκτά 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 $(0_R, \ldots, 0_R)$. Εξάλλου, δοθέντων n αυθαιρέτως επιλεγμένων δακτυλίων $R_1, R_2, \ldots, R_n$ μπορούμε να ορίσουμε τη δομή ενός δακτυλίου επί τού *καρτεσιανού* ή (*εξωτερικού*) *ευθέος γινομένου* τους

$$\prod_{j=1}^{n} R_j := R_1 \times \cdots \times R_n \tag{1.1}$$

[3] Όταν $m = 1$, έχουμε $[0]_m = [1]_m$.

με τις ανάλογες πράξεις κατά παράγοντες. Ο δακτύλιος (1.1) είναι μεταθετικός εάν και μόνον εάν καθένας των παραγόντων του είναι μεταθετικός. Επιπροσθέτως, ο (1.1) έχει μοναδιαίο στοιχείο εάν και μόνον εάν καθένας των παραγόντων του έχει μοναδιαίο στοιχείο. (Μάλιστα, όταν ο (1.1) έχει μοναδιαίο στοιχείο, τότε αυτό είναι το $(1_{R_1}, \ldots, 1_{R_n})$.) Κατ' αναλογίαν, εάν η $(R_j)_{j\in J}$ είναι μια μη κενή οικογένεια δακτυλίων, μπορούμε να ορίσουμε τη δομή δακτυλίου επί τού $\prod_{j\in J} R_j$ μέσω των πράξεων

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

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

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

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

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

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

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

(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.

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

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

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

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

(iv) *Για οιαδήποτε στοιχεία* $a_1, \ldots, a_n, b_1, \ldots, b_m$ *τού* R *έχουμε*

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

(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 ως προς τον n. Για $n = 1$ η ανωτέρω ισότητα γράφεται ως

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

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

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

Εφαρμόζοντας εκ νέου την επιμεριστική ιδιότητα, σε συνδυασμό με την επαγωγική

μας υπόθεση, λαμβάνουμε

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

(v) Τούτο έπεται άμεσα από το (iv).

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

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

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

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

1.1.7 Πρόταση. (Διωνυμικοί τύποι) *Για κάθε μη αρνητικό ακέραιο αριθμό n ας συμβολίσουμε ως $n! = 1 \cdot 2 \cdots n$ 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 δακτύλιος με μοναδιαίο στοιχείο, ο n ένας παγιωμένος φυσικός αριθμός, και (για κάποιον $\nu \in \mathbb{N}$) τα $a, b, a_1, a_2, \ldots, a_\nu$, στοιχεία τού R, έχουμε*:

(i) *Εάν $ab = ba$, τότε*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k} \tag{1.2}$$

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

$$(a_1 + a_2 + \cdots + a_\nu)^n = \sum \frac{n!}{(i_1!)\,(i_2!)\cdots(i_\nu!)}\, a_1^{i_1}\, a_2^{i_2} \cdots a_\nu^{i_\nu} \tag{1.3}$$

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:

$$\binom{n}{j} + \binom{n}{j+1} = \binom{n+1}{j+1} \tag{1.4}$$

για κάθε $j, 0 \leq j < n$, και θα εργασθούμε με μαθηματική επαγωγή ως προς τον n. Για $n = 0$ η (1.2) είναι προφανής. Υποθέτοντας ότι η (1.2) είναι αληθής για κάποιον $n \geq 1$, λαμβάνουμε μέσω τής επιμεριστικής ιδιότητας:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k\,b^{n-k}\\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}\,b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k\,b^{n-k+1} \qquad [\text{επειδή } ab=ba]\\
&= \binom{n}{n}a^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}\,a^{k+1}\,b^{n-k} + \sum_{k=1}^{n}\binom{n}{k}\,a^k\,b^{n-k+1} + \binom{n}{0}b^{n+1}\\
&= \binom{n+1}{n+1}a^{n+1} + \sum_{j=0}^{n-1}\binom{n}{j}\,a^{j+1}\,b^{(n+1)-(j+1)} +\\
&+ \sum_{j=0}^{n-1}\binom{n}{j+1}\,a^{j+1}\,b^{(n+1)-(j+1)} + \binom{n+1}{0}b^{n+1}\\
&= \binom{n+1}{n+1}a^{n+1} + \sum_{j=0}^{n-1}\left(\binom{n}{j} + \binom{n}{j+1}\right)a^{j+1}\,b^{(n+1)-(j+1)} + \binom{n+1}{0}b^{n+1}\\
&\overset{(1.4)}{=} \binom{n+1}{n+1}a^{n+1} + \sum_{j=0}^{n-1}\binom{n+1}{j+1}\,a^{j+1}\,b^{(n+1)-(j+1)} + \binom{n+1}{0}b^{n+1}\\
&= \binom{n+1}{n+1}a^{n+1} + \sum_{k=0}^{n}\binom{n+1}{k}a^k\,b^{(n+1)-k} + \binom{n+1}{0}b^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k\,b^{(n+1)-k}\,.
\end{aligned}$$

(ii) Για την απόδειξη τού τύπου (1.3) αρκεί να εφαρμόσουμε μαθηματική επαγωγή ως προς τον πληθικό αριθμό ν των προσθετέων. Για $n \in \{0,1\}$ ο (1.3) είναι προφανής, ενώ για $n = 2$ συμπίπτει με τον (1.2), αφού

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

Εάν υποθέσουμε ότι ο (1.3) είναι αληθής για κάποιον ν, τότε θα είναι αληθής και για τον $\nu+1$, διότι

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

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

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. □

1.1.8 Σημείωση. Δεδομένων των συνθηκών αμοιβαίας μεταθετικότητας των όρων μας, ανεπαίσθητες παραλλαγές των (1.2) και (1.3) παραμένουν ισχύουσες ακόμη και όταν ο δακτύλιος R *δεν* διαθέτει μοναδιαίο στοιχείο. Συγκεκριμένα, σε αυτήν την περίπτωση, μπορούμε να γράψουμε αντί τής (1.2),

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

(και, αντιστοίχως, να μην εμφανίσουμε *καθόλου* στην (1.3) τους παράγοντες που είναι υψωμένοι στη μηδενική δύναμη). Ωστόσο, θα πρέπει να έχουμε πάντοτε στο νου μας ότι, όταν ένας δακτύλιος αναφοράς R δεν διαθέτει μοναδιαίο στοιχείο, το na, όπου $n \in \mathbb{Z}$ και $a \in R$, είναι στοιχείο τού R, *χωρίς* όμως το na να υποδηλοί -εν γένει- πολλαπλασιασμό δύο στοιχείων *εντός* τού R. Αντιθέτως, όταν ο R είναι δακτύλιος με μοναδιαίο, τότε το na υποδηλοί πάντοτε πολλαπλασιασμό δύο στοιχείων εντός τού R, καθότι αυτό γράφεται ως

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

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

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

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

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

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

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

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

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

$$\begin{aligned}(a+bi) + (c+di) &:= (a+c) + (b+d)i,\\ (a+bi) \cdot (c+di) &:= (ac-bd) + (ad+bc)i,\end{aligned}$$

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

$$\boxed{\mathbb{Z}[\sqrt{m}] := \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} \subsetneqq \mathbb{C}} \tag{1.5}$$

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

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

Κατ' αναλογίαν, το

$$\boxed{\mathbb{Q}\left(\sqrt{m}\right) := \{r + s\sqrt{m} \mid r, s \in \mathbb{Q}\} \subsetneqq \mathbb{C}} \tag{1.6}$$

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:

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

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

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

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

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

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

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

1.1.13 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 $0_R \in \bigcap\limits_{j \in J} S_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $a, b \in \bigcap\limits_{j \in J} S_j$, τότε

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

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

1.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

1.2.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα στοιχείο $a \in R \setminus \{0_R\}$ καλείται **δεξιός** (και αντιστοίχως, **αριστερός**) **μηδενοδιαιρέτης** όταν υπάρχει ένα $b \in R \setminus \{0_R\}$ (αντ. $c \in R \setminus \{0_R\}$), τέτοιο ώστε $ba = 0_R$ (και αντιστοίχως, $ac = 0_R$). Ένα στοιχείο τού[4] $R \setminus \{0_R\}$ καλείται **αμφίπλευρος μηδενοδιαιρέτης** ή απλώς **μηδενοδιαιρέτης** όταν αυτό είναι ταυτοχρόνως και δεξιός και αριστερός μηδενοδιαιρέτης. Το σύνολο όλων των μηδενοδιαιρετών ενός δακτυλίου R θα συμβολίζεται ως $\mathrm{Zdv}(R)$.

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

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

διότι

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

και

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

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

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

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

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 την κάπως γενικότερη πρόταση 1.2.17. □

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

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

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

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

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

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

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

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

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

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

1.2.7 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο[5] $1_R \neq 0_R$. Ένα στοιχείο $a \in R$ καλείται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **αντιστρέψιμο** όταν $\exists b \in R$ (και αντιστοίχως, $\exists c \in R$), τέτοιο ώστε $ba = 1_R$ (και αντιστοίχως,

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

$ac = 1_R$). 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 μη τετριμμένου δακτυλίου R με μοναδιαίο στοιχείο θα συμβολίζεται ως $R^\times$.

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

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

1.2.9 Συμβολισμός. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω $a \in R^\times$. Τότε υπάρχει κάποιο στοιχείο τού R, ας το πούμε b, τέτοιο ώστε $ba = 1_R = ab$ (επί τη βάσει τού ορισμού 1.2.7 και τής προτάσεως 1.2.8). Το b είναι *το μόνο* στοιχείο τού R που πληροί αυτήν την ιδιότητα, διότι για οιοδήποτε $b' \in R$ με $b'a = 1_R = ab'$ έχουμε $b = b'$ (αφού το b είναι εξ αριστερών αντίστροφο και το b' εκ δεξιών αντίστροφο τού a και τανάπαλιν). Αυτό το b καλείται **αντίστροφο στοιχείο τού** a και θα συμβολίζεται εφεξής ως a^{-1}. (Προφανώς, $1_R^{-1} = 1_R$ και $\{\pm 1_R\} \subseteq R^\times$, $0_R \notin R^\times$.) Επίσης, για κάθε $a \in R^\times$ και κάθε $n \in \mathbb{N}$, θα γράφουμε εν συντομία $a^{-n} := (a^{-1})^n$ (πρβλ. 1.1.6).

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

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

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

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

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

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

(ii) Άλλοτε η $R^\times$ έχει *πεπερασμένη* τάξη, όπως στην περίπτωση θεωρήσεως τού δακτυλίου $R = \mathbb{Z}_m$, $m \geq 2$, με

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid 1 \leq k \leq m-1,\ \ \text{μκδ}\,(k, m) = 1\}$$

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

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

είναι άπειρη αριθμήσιμη (βλ. σημείωση 5.2.41) και η $(\mathrm{Mat}_{n\times n}(\mathbb{R}))^\times$ άπειρη υπεραριθμήσιμη (βλ. πρόταση 1.2.13).

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

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

$$1_R = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \neq \left(\begin{array}{cc} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{array} \right) = 1_S$$

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

$$\left(\begin{array}{cc} x & x \\ x & x \end{array} \right) \left(\begin{array}{cc} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{array} \right) = 1_S = \left(\begin{array}{cc} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{array} \right) \left(\begin{array}{cc} x & x \\ x & x \end{array} \right),$$

οπότε

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

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

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

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

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

ΑΠΟΔΕΙΞΗ. Εάν $\mathbf{A} \in (\mathrm{Mat}_{n\times n}(R))^\times$, τότε υπάρχει το αντίστροφο στοιχείο $\mathbf{A}^{-1} \in \mathrm{Mat}_{n\times n}(R)$ με

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_n.$$

Λαμβάνοντας υπ' όψιν τις ιδιότητες των οριζουσών $n \times n$ πινάκων με τις εγγραφές τους ειλημμένες από τον R (βλ. τα (i) και (vii) τής ασκήσεως **1-13**) έχουμε

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

δηλαδή ότι $\det(\mathbf{A}) \in R^\times$. Και αντιστρόφως· εάν $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ 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 $\mathbf{C} \in \mathrm{Mat}_{n\times n}(R)$, 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

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

(βλ. (1.14) στο (x) τής ασκήσεως **1-13**) 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 $\mathbf{A} \in (\mathrm{Mat}_{n\times n}(R))^\times$. □

1.2.14 Σημείωση. (i) Η ομάδα $(\mathrm{Mat}_{n\times n}(R))^\times$ συμβολίζεται συνήθως ως $\mathrm{GL}_n(R)$ και ονομάζεται **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

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

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

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

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

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

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

και

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

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 λοιπές εγκλειστικές σχέσεις είναι προφανείς. □

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

(ii) Κάθε μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $R^\times = R \smallsetminus \{0_R\}$ καλείται **διαιρετικός**[6] **δακτύλιος** ή **στρεβλό σώμα**[7]**.**

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

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

(ii) Έστω

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

ο υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ 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[8]

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

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

[7] 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 $0_R (\neq 1_R)$).

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

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

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

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

$$\left(\begin{array}{cc} a+bi & c+di \\ -c+di & a-bi \end{array} \right) \neq \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right),$$

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

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

ανήκει στην ομάδα $\mathbb{H}_{\mathbb{R}}^{\times}$. Άρα ο $\mathbb{H}_{\mathbb{R}}$ αποτελεί έναν *διαιρετικό δακτύλιο*[9], ο οποίος ονομάζεται **δακτύλιος των τετρανίων**[10] **υπεράνω τού σώματος** $\mathbb{R}$.

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

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

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

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

1.2.23 Παράδειγμα. Υπάρχουν ακέραιες περιοχές που δεν είναι σώματα. Τα απλούστερα παραδείγματα μας τα παρέχουν ο δακτύλιος $\mathbb{Z}$ των ακεραίων (με τις

[9] 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 $\mathbb{R}$.

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

συνήθεις πράξεις), αφού $\mathrm{Zdv}(\mathbb{Z}) = \varnothing$ και $\mathbb{Z}^\times = \{-1, +1\} \subsetneqq \mathbb{Z}\setminus\{0\}$, και ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. άσκηση **1-36**), αφού

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

Από την άλλη μεριά, για *πεπερασμένους* μεταθετικούς δακτυλίους με μοναδιαίο στοιχείο $1_R \neq 0_R$ οι έννοιες ακεραία περιοχή και σώμα ταυτίζονται (βλ. πρόταση 1.2.26).

1.2.24 Σημείωση. Εάν ο R είναι μια ακεραία περιοχή και ο S υποδακτύλιος τού R με μοναδιαίο στοιχείο $1_S = 1_R$ 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 **1-25**).

1.2.25 Σημείωση. Εάν το L είναι ένα σώμα και το K ένας υποδακτύλιος τού L με μοναδιαίο στοιχείο $1_L = 1_K$ 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 οι οποίοι στερούνται τετραγώνων, τα λεγόμενα **τετραγωνικά αριθμητικά σώματα** $\mathbb{Q}(\sqrt{m})$ (με τις αυτονόητες πράξεις προσθέσεως και πολλαπλασιασμού, βλ. άσκηση **1-37**) 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 $m \in \mathbb{Z}, m \leq -1$.

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

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

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

(i) *Ο m είναι πρώτος αριθμός.*

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

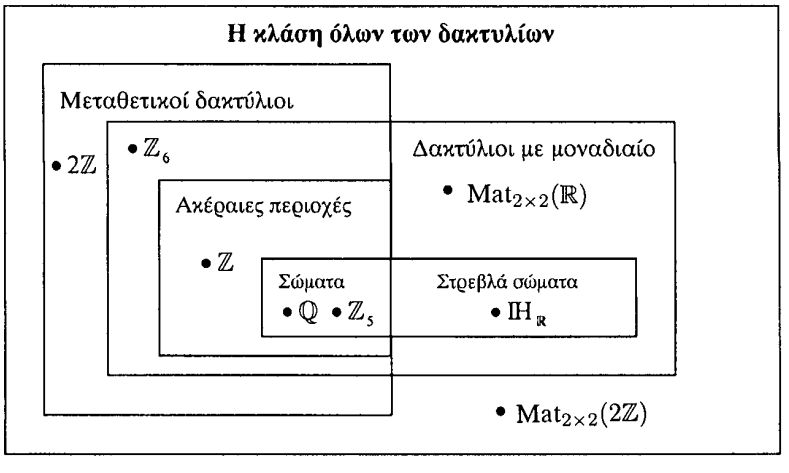
(iii) *Ο $\mathbb{Z}_m$ αποτελεί ένα σώμα.*

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

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

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

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



1.3 ΔΑΚΤΥΛΙΟΙ ΠΟΛΥΩΝΥΜΩΝ ΚΑΙ ΕΠΙΤΥΠΩΝ ΔΥΝΑΜΟΣΕΙΡΩΝ

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

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

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

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

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

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

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0, \; \forall m \in \mathbb{N}_0. \tag{1.7}$$

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

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

παρατηρούμε ότι, βάσει των ως άνω πράξεων,

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

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

και, γενικότερα,

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

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

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

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

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

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

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

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

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

1.3.3 Σημείωση. Εκ των ανωτέρω συμπεραίνουμε ότι δυο επίτυπες δυναμοσειρές

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

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

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

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

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

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

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

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

τότε λέμε ότι ο αριθμός $\mathrm{ord}(f(\mathsf{X})) := n$ είναι **η τάξη** τής επίτυπης δυναμοσειράς $f(\mathsf{X})$ και το a_0 **ο σταθερός όρος** τής $f(\mathsf{X})$. Στην περίπτωση όπου $f(\mathsf{X}) = 0_{R[\![\mathsf{X}]\!]}$ είναι η **μηδενική επίτυπη δυναμοσειρά**, θέτουμε εξ ορισμού $\mathrm{ord}(f(\mathsf{X})) := \infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[11]: $\infty > n, \;\; \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο η τάξη των επίτυπων δυναμοσειρών μπορεί να εκληφθεί ως μια απεικόνιση

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

1.3.5 Λήμμα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Για οιεσδήποτε επίτυπες δυναμοσειρές $f(\mathsf{X}), g(\mathsf{X}) \in R[\![\mathsf{X}]\!] \setminus \{0_{R[\![\mathsf{X}]\!]}\}$ ισχύουν τα εξής*:

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

(ii) $\mathrm{ord}(f(\mathsf{X}) \cdot g(\mathsf{X})) \geq \mathrm{ord}(f(\mathsf{X})) + \mathrm{ord}(g(\mathsf{X}))$.

(iii) *Εάν* $\mathrm{ord}(f(\mathsf{X})) \neq \mathrm{ord}(g(\mathsf{X}))$, *τότε*

$$\mathrm{ord}\,(f(\mathsf{X}) + g(\mathsf{X})) = \min\{\mathrm{ord}\,(f(\mathsf{X})), \mathrm{ord}(g(\mathsf{X}))\}.$$

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

$$\mathrm{ord}\,(f(\mathsf{X}) \cdot g(\mathsf{X})) = \mathrm{ord}\,(f(\mathsf{X})) + \mathrm{ord}(g(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι

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

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

$$f(\mathsf{X}) + g(\mathsf{X}) = \sum_{i=0}^{\infty} (a_i + b_i)\, \mathsf{X}^i = \begin{cases} a_n + \displaystyle\sum_{i=n+1}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n < m \\ \displaystyle\sum_{i=n}^{\infty} (a_i + b_i)\, \mathsf{X}^i, & \text{όταν } n = m \end{cases} \tag{1.8}$$

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

οπότε[12] $\text{ord}(f(\mathsf{X})+g(\mathsf{X})) \geq n = \min\{\text{ord}(f(\mathsf{X})), \text{ord}(g(\mathsf{X}))\}$.

(ii) Βάσει τής (1.7) το γινόμενο των δύο επίτυπων δυναμοσειρών μπορεί να γραφεί ως

$$f(\mathsf{X}) \cdot g(\mathsf{X}) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) \mathsf{X}^k,$$

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ 0_R, & \text{όταν } k \leq n+m-1 \end{cases} \tag{1.9}$$

Κατά συνέπειαν[13], $\text{ord}(f(\mathsf{X}) \cdot g(\mathsf{X})) \geq n+m = \text{ord}(f(\mathsf{X})) + \text{ord}(g(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n < m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (1.8) έπεται ότι

$$\text{ord}\left(f(\mathsf{X}) + g(\mathsf{X})\right) = n = \min\{\text{ord}\left(f(\mathsf{X})\right), \text{ord}(g(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m \neq 0_R$, λαμβάνουμε $\text{ord}(f(\mathsf{X}) \cdot g(\mathsf{X})) = \text{ord}(f(\mathsf{X})) + \text{ord}(g(\mathsf{X}))$ από την (1.9). □

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

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

τότε λέμε ότι ο αριθμός $\deg\left(f(\mathsf{X})\right) := n$ είναι **ο βαθμός** τού πολυωνύμου $f(\mathsf{X})$, το a_0 **ο σταθερός όρος** τού $f(\mathsf{X})$ και ο $\text{LC}(f(\mathsf{X})) := a_n$ ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού $f(\mathsf{X})$. Όταν $\text{LC}(f(\mathsf{X})) = 1_R$, τότε το $f(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου $f(\mathsf{X}) = 0_{R[\mathsf{X}]}$ είναι το **μηδενικό πολυώνυμο**, θέτουμε εξ ορισμού $\deg(f(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[14]: $-\infty < n, \ \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

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

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

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

[13] Αυτή ισχύει ως *γνήσια* ανισότητα εάν και μόνον εάν $a_n b_m = 0_R$.

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

1.3.7 Λήμμα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Για οιαδήποτε πολυώνυμα $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ ισχύουν τα εξής:*

(i) $\deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) \leq \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}$.

(ii) $\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) \leq \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$.

(iii) *Εάν* $\deg\left(f(\mathsf{X})\right) \neq \deg(g(\mathsf{X}))$, *τότε*

$$\deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) = \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}.$$

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

$$\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι

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

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

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

$$f(\mathsf{X}) + g(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{1.10}$$

οπότε $\deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) \leq n = \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}$.

(ii) Βάσει τής (1.7) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

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

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0_R, & \text{όταν } k \geq n+m+1 \end{cases} \tag{1.11}$$

Κατά συνέπειαν, $\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) \leq n + m = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (1.10) έπεται ότι

$$\deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) = n = \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m = \mathrm{LC}(f(\mathsf{X}))\cdot \mathrm{LC}(g(\mathsf{X})) \neq 0_R$, από την ισότητα (1.11) λαμβάνουμε $\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$. □

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

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

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

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

που σημαίνει ότι

$$0 = \deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) < \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})) = 2.$$

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

$$\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$$

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

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

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

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

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

$$\operatorname{LC}(f(\mathsf{X})) \cdot \operatorname{LC}(g(\mathsf{X})) \neq 0_R,$$

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

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

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

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

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

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

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

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

έχουμε

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

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

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

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

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

Θέτοντας $g(\mathsf{X}) := \sum\limits_{i=0}^{\infty} b_i \mathsf{X}^i$, λαμβάνουμε $f(\mathsf{X})g(\mathsf{X}) = 1_R$ και ο ισχυρισμός είναι αληθής. □

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

$$\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$$

και

$$K\left[\mathsf{X}\right]^{\times} = K^{\times} = K \setminus \{0_K\} = \left\{ f\left(\mathsf{X}\right) \in K[\mathsf{X}] \mid \deg(f(\mathsf{X})) = 0 \right\}.$$

(ii) *Εάν* $f(\mathsf{X}), g(\mathsf{X}) \in K[\![\mathsf{X}]\!] \setminus \{0_{K[\![\mathsf{X}]\!]}\}$, *τότε*

$$\operatorname{ord}\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \operatorname{ord}\left(f(\mathsf{X})\right) + \operatorname{ord}(g(\mathsf{X}))$$

και

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

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

$$f(\mathsf{X}) = \mathsf{X}^{\operatorname{ord}(f(\mathsf{X}))} h(\mathsf{X}),$$

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

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

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

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

1.3.11 Σημείωση. Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «απεικονίσεις» (επειδή εκεί γίνεται κυρίως χρήση των δακτυλίων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντες* δακτυλίους R με μοναδιαίο στοιχείο, κάτι τέτοιο *δεν* είναι εν γένει αληθές. Εάν

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],$$

η **απεικόνιση η επαγομένη από το** $f(\mathsf{X})$ είναι εξ ορισμού η

$$\mathfrak{v}_{f(\mathsf{X})} : R \longrightarrow R, \quad r \longmapsto \mathfrak{v}_{f(\mathsf{X})}(r) := f(r) := \sum_{i=1}^{n} a_i r^i.$$

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

$$f\left(\mathsf{X}\right) = [1]_3\, \mathsf{X} + [1]_3\, \mathsf{X}^3, \quad g(\mathsf{X}) = [2]_3\, \mathsf{X},$$

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

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

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

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

1.3.12 Ορισμός. (i) Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Ο δακτύλιος $(R[\![\mathsf{X}_1]\!])\,[\![\mathsf{X}_2]\!]$ των επίτυπων δυναμοσειρών μίας μεταβλητής X_2 με συντελεστές ειλημμένους από τον $R[\![\mathsf{X}_1]\!]$ καλείται **δακτύλιος επίτυπων δυναμοσειρών δύο (ανεξαρτήτων) μεταβλητών** X_1 **και** X_2 με συντελεστές ειλημμένους από τον R και συμβολίζεται ως $R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$. Κάθε στοιχείο $f(\mathsf{X}_1, \mathsf{X}_2) \in R[\![\mathsf{X}_1, \mathsf{X}_2]\!]$ είναι τής μορφής

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

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

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

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

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

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

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

1.4 Η ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΤΩΝ ΔΑΚΤΥΛΙΩΝ

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

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

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 $\text{χαρ}(R)$.

1.4.2 Παραδείγματα. (i) Οι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ έχουν χαρακτηριστική 0.

(ii) Ο $\mathbb{Z}_m$ έχει χαρακτηριστική m.

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

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

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

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

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

δηλαδή κάτι που θα αντέφασκε προς το γεγονός ότι ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $na = 0_R$ για κάθε $a \in R$.

"$\Longleftarrow$" Εάν ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίον $n \cdot 1_R = 0_R$, τότε για κάθε $a \in R$ έχουμε

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

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

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

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

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

ΑΠΟΔΕΙΞΗ. Έστω ότι $\text{χαρ}(R) = n \neq 0$. Υποθέτουμε πως ο n είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $n = kl$ δύο φυσικών αριθμών k και l, όπου $1 < k, l < n$. Τότε $0_R = n \cdot 1_R = (kl) \cdot 1_R = (k \cdot 1_R)(l \cdot 1_R)$, και επειδή ο R δεν διαθέτει μηδενοδιαιρέτες λαμβάνουμε

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

πράγμα που αντιφάσκει προς το γεγονός ότι ο n είναι ο *ελάχιστος* φυσικός αριθμός με αυτήν την ιδιότητα (βλ. πρόταση 1.4.3). Άρα τελικώς ο n οφείλει να είναι πρώτος αριθμός. □

1.4.6 Πρόταση. *Έστω R μια ακεραία περιοχή.*

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

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

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

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

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

(ii) Εάν $\text{χαρ}(R) = p$ (p πρώτος) και εάν θεωρήσουμε ένα $a \in R \setminus \{0_R\}$, τότε από τον ορισμό τής χαρακτηριστικής τού R προκύπτει ότι $\text{ord}(a) \leq p$. Όμως η ισότητα $0_R = \text{ord}(a)\, a = (\text{ord}\,(a) \cdot 1_R)\, a$ 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 1.4.3. Συνεπώς, $\text{ord}(a) = p$. □

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

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

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

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

Ασκήσεις

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

(i) $n(ab)=(na)b$, για κάθε $n\in\mathbb{Z}$ και κάθε $(a,b)\in R^2$.

(ii) $n(ab)=a(nb)$, για κάθε $n\in\mathbb{Z}$ και κάθε $(a,b)\in R^2$.

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

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

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

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

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

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

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

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

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

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

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

(v) Για κάθε φυσικό αριθμό $n\geq 2$,

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

1-3. Έστω $(R,+,\cdot)$ ένας δακτύλιος. Λέμε ότι ο δακτύλιος $(R,+,*)$ ο οριζόμενος επί τού συνόλου R, με την ίδια την "$+$" ως πράξη προσθέσεως και την

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

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

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

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

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

1-4. Έστω R ένας δακτύλιος για τον οποίο ισχύει η ισότητα

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

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

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

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

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

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

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

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

1-7. Έστω M ένα μη κενό σύνολο και έστω $\mathfrak{P}(M)$ το δυναμοσύνολό του. Να αποδειχθεί ότι η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$, όπου

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

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

1-8. Έστω p πρώτος αριθμός και $Q_p := \left\{ \left[x^2\right]_p \;\middle|\; [x]_p \in \mathbb{Z}_p \right\}$ το σύνολο των τετραγώνων των στοιχείων τού $\mathbb{Z}_p$.

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

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

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

1-9. Έστω p πρώτος αριθμός. Να αποδειχθεί ότι κάθε στοιχείο τού $\mathbb{Z}_p$ *μπορεί να παρασταθεί ως άθροισμα τετραγώνων* δύο στοιχείων τού $\mathbb{Z}_p$. (*Υπόδειξη*: Να γίνει κατάλληλη χρήση τής ασκήσεως **1-8**.)

1-10. Να αποδειχθεί η πρόταση 1.1.10.

1-11. Για οιονδήποτε πρώτο αριθμό p ορίζουμε το σύνολο

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

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

1-12. Εάν η $(G,+)$ είναι μια προσθετική αβελιανή ομάδα, να αποδειχθεί ότι η τριάδα $(\mathrm{End}(G),+,\circ)$, όπου $\mathrm{End}(G)$ το σύνολο των ενδομορφισμών τής G, "$+$" η συνήθης (κατά σημείο) πρόσθεση και "$\circ$" η συνήθης πράξη τής συνθέσεως απεικονίσεων, αποτελεί έναν δακτύλιο με την id_G ως μοναδιαίο του στοιχείο.

1-13. Εάν ο n είναι ένας φυσικός αριθμός και ο R ένας μεταθετικός μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, τότε **η ορίζουσα** $\det(\mathbf{A})$ ενός πίνακα

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

ορίζεται μέσω τού τύπου τού Leibniz:

$$\boxed{\det(\mathbf{A}) := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma)\, a_{1\,\sigma(1)}\, a_{2\,\sigma(2)} \cdots a_{n\,\sigma(n)}} \tag{1.12}$$

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

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

Να αποδειχθούν τα ακόλουθα:

(i) $\det(\mathbf{I}_n) = 1_R$,

(ii) Έστω $r \in R$. Εάν ο πίνακας $\mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$ προκύπτει από τον πίνακα $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ύστερα από πολλαπλασιασμό όλων των εγγραφών τής i-οστής γραμμής (ή τής i-οστής στήλης) τού $\mathbf{A}$ με το r, όπου $i \in \{1,\ldots,n\}$, τότε

$$\det(\mathbf{B}) = r\det(\mathbf{A}).$$

Εξ αυτού έπεται ότι

$$\det(r\mathbf{A}) = r^n \det(\mathbf{A}).$$

(Εν προκειμένω, ως $r\mathbf{A}$ συμβολίζουμε τον πίνακα που προκύπτει κατόπιν *αριθμητικού πολλαπλασιασμού* τού r με τον πίνακα $\mathbf{A} = (a_{ij})_{1\leq i,j\leq n}$, ήτοι τον $r\mathbf{A} = (ra_{ij})_{1\leq i,j\leq n}$).

(iii) Εάν οι πίνακες $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathrm{Mat}_{n\times n}(R)$ διαθέτουν τις ίδιες εγγραφές σε κάθε γραμμή τους που είναι διάφορη τής j-οστής (για κάποιο παγιωμένο $j \in \{1, \ldots, n\}$) και, επιπροσθέτως, η j-οστή γραμμή τού $\mathbf{C}$ ισούται με το άθροισμα τής j-οστής γραμμής τού $\mathbf{A}$ και τής j-οστής γραμμής τού $\mathbf{B}$, τότε

$$\det(\mathbf{C}) = \det(\mathbf{A}) + \det(\mathbf{B}).$$

(iv) Υποθέτοντας ότι $n > 1$ και ότι η k-αστή γραμμή (και, αντιστοίχως, k-αστή στήλη) ενός πίνακα $\mathbf{B} = (b_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(R)$ ισούται με την l-οστή του γραμμή (και, αντιστοίχως, την l-οστή του στήλη), όπου $1 \leq k < l \leq n$, έχουμε

$$\det(\mathbf{B}) = 0_R.$$

(v) Έστω ότι $n > 1$ και $k, l \in \mathbb{N}$ με $1 \leq k, l \leq n$ και $k \neq l$, και ότι $r \in R$. Εάν ο πίνακας $\mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$ προκύπτει από τον πίνακα $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ύστερα από πρόσθεση τού γινομένου τής k-αστής γραμμής (και, αντιστοίχως, τής k-αστής στήλης) με το r στην l-οστή γραμμή (και, αντιστοίχως, l-οστή στήλη) τού $\mathbf{A}$, τότε

$$\det(\mathbf{B}) = \det(\mathbf{A}).$$

(vi) Εάν $n > 1$ και $k, l \in \mathbb{N}$ με $1 \leq k, l \leq n$, $k \neq l$, και εάν ο $\mathbf{B} \in \mathrm{Mat}_{n\times n}(R)$ προκύπτει από τον πίνακα $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ύστερα από εναλλαγή τής k-αστής του γραμμής (και, αντιστοίχως, τής k-αστής του στήλης) με την l-οστή του γραμμή (και, αντιστοίχως, με την l-οστή του στήλη), τότε

$$\det(\mathbf{B}) = -\det(\mathbf{A}).$$

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

$$\boxed{\det(\mathbf{A})\det(\mathbf{B}) = \det(\mathbf{AB}).} \tag{1.13}$$

(viii) Έστω ότι $n > 1$ και $i, j \in \mathbb{N}$ με $1 \leq i, j \leq n$. Εάν ο πίνακας

$$\mathbf{B}_{ij} \in \mathrm{Mat}_{(n-1)\times(n-1)}(R)$$

είναι ο «ελάσσων πίνακας» ο σχηματιζόμενος από τον $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$ ύστερα από τη διαγραφή τής i-οστής του στήλης και τής j-οστής του γραμμής, τότε το στοιχείο

$$\mathrm{cof}_{ij}(\mathbf{A}) := (-1)^{i+j} \det(\mathbf{B}_{ij})$$

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

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

ο πίνακας ο προσαρτημένος στον A. Επειδή

$$\mathrm{cof}_{ij}(\mathbf{A}) = \det \begin{pmatrix} a_{11} & \cdots & a_{1\,j-1} & a_{1\,j} & a_{1\,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-1\,1} & \cdots & a_{i-1\,j-1} & a_{i-1\,j} & a_{i-1\,j+1} & \cdots & a_{i-1\,n} \\ 0_R & \cdots & 0_R & 1_R & 0_R & \cdots & 0_R \\ a_{i+1\,1} & \cdots & a_{i+1\,j-1} & a_{i+1\,j} & a_{i+1\,j+1} & \cdots & a_{i+1\,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n\,j-1} & a_{n\,j} & a_{n\,j+1} & \cdots & a_{nn} \end{pmatrix},$$

η ορίζουσα (1.12) τού $\mathbf{A}$ εκφράζεται μέσω των συμπαραγόντων του ως ακολούθως:

$$\det(\mathbf{A}) = \sum_{j=1}^{n} a_{kj}\,\mathrm{cof}_{kj}(\mathbf{A}) = \sum_{i=1}^{n} a_{ik}\,\mathrm{cof}_{ik}(\mathbf{A}), \quad \forall k \in \{1,\dots,n\}.$$

(ix) Έστω ότι $n > 1$ και $k, l \in \mathbb{N}$ με $1 \le k, l \le n$. Τότε

$$\sum_{j=1}^{n} a_{kj}\,\mathrm{cof}_{lj}(\mathbf{A}) = \begin{cases} 0_R, & \text{όταν } k \ne l, \\ \det(\mathbf{A}), & \text{όταν } k = l, \end{cases}$$

και

$$\sum_{i=1}^{n} a_{ik}\,\mathrm{cof}_{il}(\mathbf{A}) = \begin{cases} 0_R, & \text{όταν } k \ne l, \\ \det(\mathbf{A}), & \text{όταν } k = l. \end{cases}$$

(x) Για οιονδήποτε φυσικό αριθμό n ισχύουν οι ισότητες

$$\boxed{\det(\mathbf{A})\ \mathbf{I}_n = \mathbf{A}\,\mathbf{adj}(\mathbf{A}) = \mathbf{adj}(\mathbf{A})\,\mathbf{A}.} \tag{1.14}$$

1-14. Έστω R ένας δακτύλιος. Ως **κέντρο** τού R ορίζεται το σύνολο

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

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

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

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

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

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

1-15. Έστω R ένας δακτύλιος για τον οποίο ισχύει $r^2 + r \in Z(R)$ για κάθε $r \in R$. Να αποδειχθεί ότι ο R είναι μεταθετικός.

1-16. Εάν τα R και S είναι δυο ακέραιες περιοχές (και, αντιστοίχως, δυο σώματα), είναι και το καρτεσιανό τους γινόμενο $R \times S$ (με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού, βλ. 1.1.4 (v)) ακεραία περιοχή (και, αντιστοίχως, σώμα);

1-17. Για οιοδήποτε $\varepsilon \in \mathbb{R}_{>0}$ ορίζουμε το $U_\varepsilon := \{\xi \mid \xi \in \mathbb{R},\ |\xi| < \varepsilon\}$, καθώς και τα σύνολα

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

Να αποδειχθεί ότι κάθε μέλος τής ακολουθίας διαδοχικώς εγκλειομένων συνόλων

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

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

1-18. Έστω S ένας υποδακτύλιος ενός δακτυλίου R. Εάν αμφότεροι οι S και R διαθέτουν μοναδιαίο στοιχείο και $1_S \neq 1_R$, να αποδειχθεί ότι το 1_S είναι ένας μηδενοδιαιρέτης εντός τού R.

1-19. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Να αποδειχθούν τα ακόλουθα:

(i) $(a^{-1})^n = (a^n)^{-1}$, $a^n = \left(a^{-1}\right)^{-n}$, για κάθε $a \in R^\times$ και $n \in \mathbb{Z}$ (βλ. 1.2.9).

(ii) Εάν $a, b \in R^\times$ και $ab = ba$, τότε

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

για κάθε $(m, n) \in \mathbb{Z}^2$ (βλ. 1.2.9).

1-20. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Υποθέτοντας την ύπαρξη δύο στοιχείων $a, b \in R$, για τα οποία ισχύουν οι ισότητες

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

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

1-21. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Υποθέτοντας ότι τα στοιχεία $x, y \in R$ είναι εκ δεξιών αντίστροφα ενός $u \in R$ (ήτοι ότι $ux = uy = 1_R$), να αποδειχθεί (i) ότι *και* το $xu + y - 1_R$ είναι ένα εκ δεξιών αντίστροφο τού u, και (ii) ότι το u διαθέτει *άπειρα* εκ δεξιών αντίστροφα όταν $x \neq y$.

1-22. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν το $a \in R$ είναι ένα μηδενοδύναμο στοιχείο τού R, να αποδειχθεί ότι το $1_R + a$ είναι αντιστρέψιμο.

1-23. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και έστω τυχόν $x \in R$. Να αποδειχθούν τα ακόλουθα:

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

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

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

1-24. Εάν $n \in \mathbb{N}$ και οι $R_1, \ldots, R_n$ είναι δακτύλιοι με μοναδιαίο στοιχείο, να αποδειχθεί ότι

$$(R_1 \times \cdots \times R_n)^\times = R_1^\times \times \cdots \times R_n^\times.$$

1-25. Έστω το σύνολο $R := \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$ εφοδιασμένο με τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού ρητών αριθμών. Να αποδειχθούν τα ακόλουθα:

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

(ii) Το R είναι ακεραία περιοχή.

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

1-26. Έστω m ένας φυσικός αριθμός ≥ 2 και έστω

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

Να αποδειχθούν τα ακόλουθα:

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

(ii) Ο R δεν είναι μεταθετικός.

(iii) Ισχύει η αμφίπλευρη συνεπαγωγή

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

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

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

1-27. Έστω

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

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

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

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

1-28. Ένα στοιχείο a ενός δακτυλίου R καλείται **ταυτοδύναμο** όταν $a^2 = a$. Να αποδειχθούν τα ακόλουθα:

(i) Έστω R τυχών δακτύλιος. Κάθε ταυτοδύναμο στοιχείο $a \in R\smallsetminus\{0_R\}$ είναι μη μηδενοδύναμο.

(ii) Εάν ο R είναι μια ακεραία περιοχή, τότε το μόνο ταυτοδύναμο στοιχείο $a \in R\smallsetminus\{0_R\}$ είναι το μοναδιαίο στοιχείο 1_R.

(iii) Το άθροισμα $a + b$ δυο ταυτοδύναμων στοιχείων a, b ενός δακτυλίου R με μοναδιαίο στοιχείο είναι ταυτοδύναμο εάν και μόνον εάν $ab = ba$ και $2ab = 0_R$.

(iv) Η διαφορά $a - b$ δυο ταυτοδύναμων στοιχείων a, b ενός δακτυλίου R με μοναδιαίο στοιχείο είναι ταυτοδύναμη εάν και μόνον εάν $ab = ba$ και $2(1_R - a)b = 0_R$.

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

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

είναι ταυτοδύναμα.

1-29. Να προσδιορισθεί (i) το σύνολο $\mathrm{Nil}(\mathbb{Z}_m)$ των μηδενοδύναμων στοιχείων και (ii) το σύνολο των ταυτοδύναμων στοιχείων τού $\mathbb{Z}_m$ για οιονδήποτε φυσικό αριθμό $m \geq 2$.

1-30. Είναι ο δακτύλιος $\mathcal{C}([0,1]) := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f \text{ συνεχής} \right\}$ (ως προς τις πράξεις τής κατά σημείο προσθέσεως και πολλαπλασιασμού) ακεραία περιοχή; Ποιο είναι το σύνολο $\mathrm{Nil}(\mathcal{C}([0,1]))$ των μηδενοδύναμων στοιχείων και ποιο το σύνολο των ταυτοδύναμων στοιχείων τού $\mathcal{C}([0,1])$; Ποια είναι η ομάδα $\mathcal{C}([0,1])^{\times}$;

1-31. Έστω R ένας δακτύλιος. Εάν ο R είναι μεταθετικός, να αποδειχθεί ότι το άθροισμα δύο μηδενοδύναμων στοιχείων του είναι μηδενοδύναμο. Εν συνεχεία, να προσδιορισθούν δύο μηδενοδύναμα στοιχεία τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$, το άθροισμα των οποίων δεν είναι μηδενοδύναμο.

1-32. Έστω R ένας μη τετριμμένος δακτύλιος. Υποτιθεμένου ότι η «εξίσωση»

$$ax = b$$

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

1-33. Να αποδειχθεί ότι σε κάθε στρεβλό σώμα R ισχύει η ισότητα

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

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

1-34. Έστω R ένας δακτύλιος με τουλάχιστον δύο στοιχεία. Υποθέτοντας ότι για κάθε $a \in R \setminus \{0_R\}$ υπάρχει ένα *μονοσημάντως ορισμένο* $b \in R$, τέτοιο ώστε $aba = a$, να αποδειχθούν τα ακόλουθα:

(i) Ο R δεν διαθέτει μηδενοδιαιρέτες.

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

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

(iv) Ο R είναι στρεβλό σώμα.

1-35. Εάν το K είναι ένα σώμα και το L ένα υποσύνολό του που περιέχει τουλάχιστον δύο στοιχεία, να αποδειχθεί ότι το L είναι υπόσωμα τού K εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:

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

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

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

1-36. Να αποδειχθεί λεπτομερώς ότι ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. 1.1.11 (ii)) είναι ακεραία περιοχή αλλά όχι και σώμα.

1-37. Για οιονδήποτε ακέραιο m ο οποίος δεν είναι τέλειο τετράγωνο, να αποδειχθούν τα ακόλουθα:

(i) Για οιαδήποτε στοιχεία $a+b\sqrt{m}$ και $c+d\sqrt{m}$ τού δακτυλίου $\mathbb{Z}[\sqrt{m}]$ (βλ. (1.5)) ισχύει η αμφίπλευρη συνεπαγωγή

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

(ii) Ο δακτύλιος $\mathbb{Z}[\sqrt{m}]$ (βλ. (1.5)) είναι *ακεραία περιοχή*.

(iii) Για κάθε $r+s\sqrt{m}\in\mathbb{Q}(\sqrt{m})$ (βλ. (1.6)) ισχύει η αμφίπλευρη συνεπαγωγή

$$r^2-ms^2=0 \Longleftrightarrow r=s=0.$$

(iv) Ο δακτύλιος $\mathbb{Q}(\sqrt{m})$ είναι *υπόσωμα* τού $\mathbb{C}$.

(v) Επειδή ο m γράφεται ως γινόμενο $m=m'k$ δύο μονοσημάντως ορισμένων ακεραίων m' και $k\geq 1$, όπου ο μεν m' στερείται τετραγώνων[15], ο δε k είναι τέλειο τετράγωνο, ισχύουν οι ισότητες

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

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

1-38. Να εξετασθεί εάν τα σύνολα $A:=\{a+b\sqrt[3]{2}\mid a,b\in\mathbb{Q}\}$ και

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

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

1-39. Εάν

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

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

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

1-40. Έστω R ένας μη τετριμμένος δακτύλιος χωρίς μηδενοδιαιρέτες, κάθε υποδακτύλιος τού οποίου διαθέτει μόνον πεπερασμένου πλήθους στοιχεία. Να αποδειχθεί ότι ο R είναι σώμα.

1-41. Να αποδειχθεί ότι ο σταθερός όρος οιουδήποτε πολυωνύμου $f(\mathsf{X}) \in \mathbb{Z}_4\,[\mathsf{X}]$ ισούται είτε με το $[1]_4$ είτε με το $[3]_4$. Εν συνεχεία, να αποδειχθεί ότι μεταξύ των αντιστρεψίμων στοιχείων τού δακτυλίου $\mathbb{Z}_4\,[\mathsf{X}]$ συγκαταλέγονται και πολυώνυμα θετικού βαθμού.

1-42. Έστω K ένα σώμα. Να αποδειχθεί ότι οι δακτύλιοι $K\,[\mathsf{X}]$ και $K[\![\mathsf{X}]\!]$ είναι ακέραιες περιοχές αλλά δεν είναι σώματα.

1-43. Δοθέντος ενός δακτυλίου R με μοναδιαίο στοιχείο θεωρούμε το σύνολο $R^{\mathbb{Z}}$ όλων των ακολουθιών

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

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

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

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

όπου

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

Να αποδειχθούν τα ακόλουθα:

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

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

τότε, βάσει των ως άνω πράξεων, κάθε στοιχείο

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

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

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

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

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

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

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

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

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

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

(vi) Ένα στοιχείο $f(\mathsf{X}) \in R[\mathsf{X}^{\pm 1}]$ είναι αντιστρέψιμο εάν και μόνον εάν

$$\exists a \in R^{\times} \text{ και } k \in \mathbb{Z} : f(\mathsf{X}) = a\,\mathsf{X}^k.$$

(vii) Ένα στοιχείο $f(\mathsf{X}) = \sum_{i=-n}^{\infty} a_i \mathsf{X}^i \in \mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ με $a_{-n} \neq 0_R$ είναι αντιστρέψιμο εάν και μόνον εάν $a_{-n} \in R^{\times}$.

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

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

1-44. (i) Να αποδειχθεί η πρόταση 1.4.8.

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

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

1-45. Εάν το K είναι ένα σώμα χαρακτηριστικής $p > 0$ και ο n ένας σταθερός φυσικός αριθμός, να αποδειχθεί ότι το

$$L := \{\, x \in K \mid x^{p^n} = x\}$$

είναι ένα υπόσωμα τού K.

1-46. Να προσδιορισθεί χαρακτηριστική τού δακτυλίου $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$, $m \in \mathbb{N}$, καθώς και η χαρακτηριστική τού διαιρετικού δακτυλίου $\mathbb{H}_{\mathbb{R}}$ των τετρανίων.

1-47. Να αποδειχθεί ότι η χαρακτηριστική οιασδήποτε υποπεριοχής μιας ακεραίας περιοχής R είναι ίση με τη χαρακτηριστική τής R.

1-48. Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, $\text{χαρ}(R) \notin \{1, 2\}$ και με την ομάδα $(R^\times, \cdot)$ των αντιστρεψίμων στοιχείων του κυκλική, να αποδειχθεί ότι η $(R^\times, \cdot)$ είναι πεπερασμένη τάξεως και $|R^\times| \equiv 0 \,(\mathrm{mod}\, 2)$.

1-49. Εάν τα R και S είναι δυο δακτύλιοι, να αποδειχθούν τα ακόλουθα για τον δακτύλιο $R \times S$ (βλ. 1.1.4 (v)):

(i) Εάν $\text{χαρ}(R) = m \in \mathbb{N}$ και $\text{χαρ}(R) = n \in \mathbb{N}$, τότε

$$\text{χαρ}\,(R \times S) = \text{εκπ}\,(m, n)\,.$$

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

1-50. Εάν $n \in \mathbb{N}$, ο p είναι ένας πρώτος αριθμός και ο R ένας δακτύλιος με μοναδιαίο στοιχείο χαρακτηριστικής p^n, να αποδειχθούν τα ακόλουθα:

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

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