Δημητρίου Ι. Νταή

ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΔΑΚΤΥΛΙΩΝ

Σημειώσεις Παραδόσεων

ΗΡΑΚΛΕΙΟ ΚΡΗΤΗΣ, 2013

Περιεχόμενα

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.

$\boxed{1.1}$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ισχύει (προφανώς) η αμφίπλευρη συνεπαγωγή

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

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

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

και n **στήλες**

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

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

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

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

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

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

$$\mathbf{A}\cdot\mathbf{B} := \left(\sum_{k=1}^{n} a_{i\,k}b_{k\,j}\right)_{1\leq i,j\leq n},$$

για οιουσδήποτε $\mathbf{A}=(a_{ij})_{1\leq i,j\leq n}$ και $\mathbf{B}=(b_{ij})_{1\leq i,j\leq n}\in \mathrm{Mat}_{n\times n}(R)$. 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*, *τεμαχισμένοι πίνακες*, *ελάσσονες πίνακες* κλπ. ορίζονται όπως και στη συνήθη Γραμμική Άλγεβρα. Για την εμπέδωση των απαραίτητων ιδιοτήτων των *οριζουσών πινάκων* που ανήκουν στον $\mathrm{Mat}_{n\times n}(R)$, όπου R κάποιος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, 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[6]) βάσει των συνήθων πράξεων

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

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

[6]Όταν $m=1$, έχουμε $[0]_m=[1]_m$.

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

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

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

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

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

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

με τις ανάλογες πράξεις κατά παράγοντες. Ο δακτύλιος (1.4) είναι μεταθετικός εάν και μόνον εάν καθένας των παραγόντων του είναι μεταθετικός. Επιπροσθέτως, ο (1.4) έχει μοναδιαίο στοιχείο εάν και μόνον εάν καθένας των παραγόντων του έχει μοναδιαίο στοιχείο. (Μάλιστα, όταν ο (1.4) έχει μοναδιαίο στοιχείο, τότε αυτό είναι το $(1_{R_1}, \ldots, 1_{R_n})$.) 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

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

(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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) Για την απόδειξη τού τύπου (1.6) αρκεί να εφαρμόσουμε μαθηματική επαγωγή ως προς τον πληθικό αριθμό ν των προσθετέων. Για $n \in \{0, 1\}$ ο (1.6) είναι προφανής, ενώ για $n = 2$ συμπίπτει με τον (1.5), 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 (1.6) είναι αληθής για κάποιον ν, τότε θα είναι αληθής και για τον $\nu+1$, διότι

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

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

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

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

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

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

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

1.1.9 Ορισμός. Ένα μη κενό υποσύνολο S (τού υποκειμένου συνόλου R) ενός δακτυλίου $(R, +, \cdot)$ καλείται **υποδακτύλιος** τού $(R, +, \cdot)$ όταν το S είναι κλειστό ως προς αμφότερες τις πράξεις "+" και "·" 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 $\mathbb{C}$):

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

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

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

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

$$\boxed{\mathbb{Q}(\sqrt{m}) := \{r + s\sqrt{m} \mid r, s \in \mathbb{Q}\} \subsetneqq \mathbb{C}} \tag{1.9}$$

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

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

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

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

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

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

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

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

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

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

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

1.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

1.2.1 Ορισμός. Έστω R ένας δακτύλιος. Ένα στοιχείο $a \in R\smallsetminus\{0_R\}$ καλείται **δεξιός** (και αντιστοίχως, **αριστερός**) **μηδενοδιαιρέτης** όταν υπάρχει ένα $b \in R\smallsetminus \{0_R\}$ (αντ. $c \in R\smallsetminus\{0_R\}$), τέτοιο ώστε $ba = 0_R$ (και αντιστοίχως, $ac = 0_R$). Ένα στοιχείο τού[7] $R\smallsetminus\{0_R\}$ 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

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

[7] 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!

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

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

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*

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

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 $d := \text{μκδ}(k,m) > 1$. 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. □

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 $c \in R \smallsetminus \{0\}$, 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[8] $1_R \neq 0_R$. Ένα στοιχείο $a \in R$ καλείται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **αντιστρέψιμο** όταν $\exists b \in R$ (και αντιστοίχως, $\exists c \in R$), τέτοιο ώστε $ba = 1_R$ (και αντιστοίχως, $ac = 1_R$). Ένα τέτοιο $b \in R$ (αντ. $c \in R$) λέγεται **αριστερό** (και αντιστοίχως, **δεξιό**) **αντίστροφο** 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**

[8] 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.

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

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

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

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

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 $\mathbf{A} \in \mathrm{Mat}_{n\times n}(R)$.

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

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

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

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

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

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

(βλ. (1.18) στο (x) τής ασκήσεως **1-13**) λαμβάνουμε τελικώς

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

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 $\mathrm{Nil}(R)$. (Ως **δείκτης** ενός $a \in \mathrm{Nil}(R)$ ορίζεται ο $\nu := \min\{n \in \mathbb{N} \mid a^n = 0_R\}$.)

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

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

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

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

και

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

ΑΠΟΔΕΙΞΗ. Έστω τυχόν στοιχείο $a \in \mathrm{Nil}(R) \smallsetminus \{0_R\}$. Εάν το a έχει δείκτη ν, τότε (προφανώς) $a^{\nu-1} \neq 0_R$ και

$$a^{\nu} = a^{\nu-1}\,a = a\,a^{\nu-1} = 0_R \Longrightarrow a \in \mathrm{Zdv}(R).$$

Έστω τώρα ότι $b \in \mathrm{Zdv}(R)$, δηλαδή ότι υπάρχουν $c, d \in R\smallsetminus\{0_R\}$ με $cb = bd = 0_R$. Εάν υποθέσουμε ότι $b \in R^{\times}$, τότε θα υπάρχουν στοιχεία $e, g \in R$, τέτοια ώστε $eb = bg = 1_R$. Αυτό όμως μας οδηγεί σε ένα άτοπο συμπέρασμα, αφού

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

Επομένως 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**[9].

[9] Εξ ορισμού, λοιπόν, μια ακεραία περιοχή είναι ένας μη τετριμμένος μεταθετικός δακτύλιος στον οποίο ισχύει ο νόμος τής διαγραφής (βλ. πρόταση 1.2.5).

(ii) Κάθε μη τετριμμένος δακτύλιος R με μοναδιαίο στοιχείο και $R^{\times} = R\smallsetminus\{0_R\}$ καλείται **διαιρετικός**[10] **δακτύλιος** ή **στρεβλό σώμα**[11].

(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[12]

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

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

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

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

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

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

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

---

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

[11] 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 $0_R(\neq 1_R)$).

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

ανήκει στην ομάδα $\mathbb{H}_{\mathbb{R}}^{\times}$. Άρα ο $\mathbb{H}_{\mathbb{R}}$ αποτελεί έναν *διαιρετικό δακτύλιο*[13], ο οποίος ονομάζεται **δακτύλιος των τετρανίων**[14] **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 συνήθεις πράξεις), αφού $\mathrm{Zdv}(\mathbb{Z}) = \varnothing$ και $\mathbb{Z}^{\times} = \{-1, +1\} \subsetneqq \mathbb{Z} \smallsetminus \{0\}$, και ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων τού Gauss (βλ. άσκηση **1-36**), αφού

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

Από την άλλη μεριά, για *πεπερασμένους* μεταθετικούς 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 $\mathbb{Z} \subsetneqq R \subseteq \mathbb{Q}$ (βλ. άσκηση **1-25**).

[13] 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 $\mathbb{R}$.

[14] 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.

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

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

(i) *Ο m είναι πρώτος αριθμός.*

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

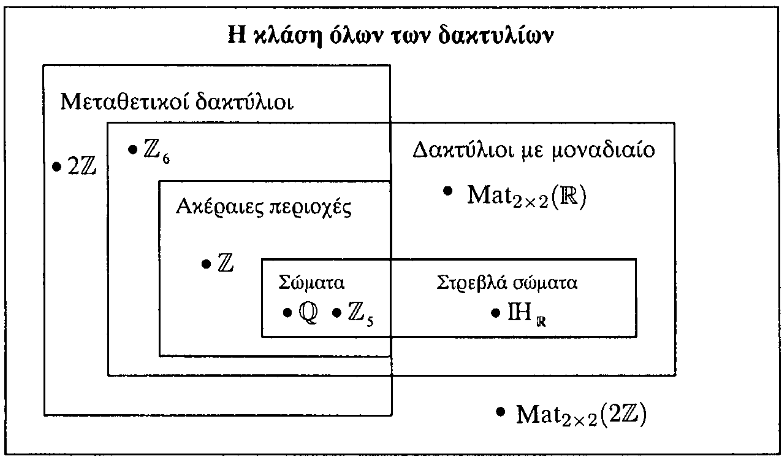
(iii) *Ο $\mathbb{Z}_m$ αποτελεί ένα σώμα.*

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

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

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

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

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

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

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

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0, \ \forall m \in \mathbb{N}_0. \tag{1.10}$$

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 **απροσδιορίστου** X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **επίτυπες δυναμοσειρές** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \ldots$ ονομάζονται **συντελεστές** των επίτυπων δυναμοσειρών.

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

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

1.3.3 Σημείωση. Εκ των ανωτέρω συμπεραίνουμε ότι δυο επίτυπες δυναμοσειρές

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

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

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

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

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

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

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

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

τότε λέμε ότι ο αριθμός $\mathrm{ord}(\varphi(\mathsf{X})) := n$ είναι **η τάξη** τής επίτυπης δυναμοσειράς $\varphi(\mathsf{X})$ και το a_0 **ο σταθερός όρος** τής $\varphi(\mathsf{X})$. Στην περίπτωση όπου $\varphi(\mathsf{X}) = 0_{R[\![\mathsf{X}]\!]}$ είναι η **μηδενική επίτυπη δυναμοσειρά**, θέτουμε εξ ορισμού $\mathrm{ord}(\varphi(\mathsf{X})) := \infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[15]: $\infty > n, \;\; \forall n \in \mathbb{N}_0$. 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 $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\![\mathsf{X}]\!]$ ισχύουν τα εξής:*

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

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

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

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

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

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

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

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

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

$$\sum_{i=0}^{\infty} (a_i + b_i)\,\mathsf{X}^i = \begin{cases} a_n \mathsf{X}^n + \sum\limits_{i=n+1}^{\infty} (a_i + b_i)\,\mathsf{X}^i, & \text{όταν } n < m, \\ \sum\limits_{i=n}^{\infty} (a_i + b_i)\,\mathsf{X}^i, & \text{όταν } n = m, \end{cases} \tag{1.11}$$

οπότε[16] $\mathrm{ord}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \geq n = \min\{\mathrm{ord}(\varphi(\mathsf{X}))\,, \mathrm{ord}(\psi(\mathsf{X}))\}$.

(ii) Βάσει τής (1.10) το γινόμενο των δύο επίτυπων δυναμοσειρών μπορεί να γραφεί ως

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

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

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

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m, \\ 0_R, & \text{όταν } k \leq n+m-1. \end{cases} \tag{1.12}$$

Κατά συνέπειαν[17], $\mathrm{ord}(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) \geq n + m = \mathrm{ord}(\varphi(\mathsf{X})) + \mathrm{ord}(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n < m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (1.11) έπεται ότι

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

(iv) Επειδή $a_n b_m \neq 0_R$, λαμβάνουμε $\mathrm{ord}(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \mathrm{ord}(\varphi(\mathsf{X})) + \mathrm{ord}(\psi(\mathsf{X}))$ από την (1.12). □

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

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

τότε λέμε ότι ο αριθμός $\deg\,(\varphi(\mathsf{X})) := n$ είναι **ο βαθμός** τού πολυωνύμου $\varphi(\mathsf{X})$, το a_0 **ο σταθερός όρος** τού $\varphi(\mathsf{X})$ και ο $\mathrm{LC}(\varphi(\mathsf{X})) := a_n$ ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού $\varphi(\mathsf{X})$. Όταν $\mathrm{LC}(\varphi(\mathsf{X})) = 1_R$, τότε το $\varphi(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ είναι το **μηδενικό πολυώνυμο**, θέτουμε εξ ορισμού $\deg(\varphi(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[18]: $-\infty < n,\ \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

$$\varphi(\mathsf{X}) + \psi(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{1.13}$$

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

(ii) Βάσει τής (1.10) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

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

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0_R, & \text{όταν } k \geq n+m+1 \end{cases} \tag{1.14}$$

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

(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (1.13) έπεται ότι

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

(iv) Επειδή $a_n b_m = \mathrm{LC}(\varphi(\mathsf{X}))\cdot \mathrm{LC}(\psi(\mathsf{X})) \neq 0_R$, από την ισότητα (1.14) λαμβάνουμε $\deg(\varphi(\mathsf{X}) \cdot \psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$. □

1.3.8 Παραδείγματα. Σημειωτέον ότι οι ανωτέρω ανισοϊσότητες μπορούν πράγματι να ισχύουν και ως αυστηρές ανισότητες.

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

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

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

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

που σημαίνει ότι

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

έχουμε

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

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

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

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

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

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

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

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

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

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

και

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

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

$$\varphi(\mathsf{X}) = \mathsf{X}^{\mathrm{ord}(\varphi(\mathsf{X}))} h(\mathsf{X}),$$

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

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

με $n := \mathrm{ord}(\varphi(\mathsf{X}))$. Θέτοντας $h(\mathsf{X}) := \sum_{i=n}^{\infty} a_i \mathsf{X}^{i-n}$ λαμβάνουμε $\varphi(\mathsf{X}) = \mathsf{X}^n h(\mathsf{X})$. 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 $K^{\times} = K \smallsetminus \{0_K\}$. □

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

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

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

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

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

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

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

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

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

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

1.3.12 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο.

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

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

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

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

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

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

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

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

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

$\boxed{1.4}$ 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 ότι ο δακτύλιος R έχει **χαρακτηριστική** 0. Η χαρακτηριστική ενός δακτυλίου R θα συμβολίζεται ως 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, χαρ$(R) = 1 \Longleftrightarrow$ ο R είναι τετριμμένος δακτύλιος.

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

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

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

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

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

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

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

οπότε 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 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 $0_R = \text{ord}(a)\, a = (\text{ord}\,(a) \cdot 1_R)\, a$ δίδει και πάλι $\text{ord}(a) \cdot 1_R = 0_R$ (διότι ο δακτύλιος R στερείται μηδενοδιαιρετών), πράγμα που σημαίνει ότι $\text{ord}(a) \geq p$ δυνάμει τής προτάσεως 1.4.3. Συνεπώς, $\text{ord}(a) = p$. □

1.4.7 Πόρισμα. *Εάν 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) $(ma)^n = m^n a^n$, 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 $R^{\rm opp}$. Να αποδειχθούν τα ακόλουθα:

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

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

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

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 $Q_p := \left\{ [a]_p^2 \ \middle| \ [a]_p \in \mathbb{Z}_p \right\}$ το σύνολο των τετραγώνων των στοιχείων τού $\mathbb{Z}_p$.

(i) Ποιος είναι ο πληθικός αριθμός 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

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

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

1-12. 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:

$$\boxed{\det(\mathbf{A}) := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma)\, a_{1\,\sigma(1)}\, a_{2\,\sigma(2)} \cdots a_{n\,\sigma(n)}} \tag{1.15}$$

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 $\mathbf{A} = (a_{ij})_{1\le i,j\le n}$, 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 $(n \times n)$-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

$$\boxed{\det(\mathbf{A}) \det(\mathbf{B}) = \det(\mathbf{A} \cdot \mathbf{B}).} \tag{1.16}$$

(viii) Έστω ότι $n > 1$. Θέτουμε για $i, j \in \mathbb{N}$ με $1 \leq i, j \leq n$,

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

Ο $\mathbf{A}'_{ij}$ είναι ο «ελάσσων πίνακας» ο σχηματιζόμενος από τον $\mathbf{A}$ ύστερα από τη διαγραφή τής i-οστής του γραμμής και τής j-οστής του στήλης. Το στοιχείο

$$\mathrm{cof}_{ij}(\mathbf{A}) := (-1)^{i+j} \det\left(\mathbf{A}'_{ij}\right) \in R \tag{1.17}$$

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

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

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

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

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

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

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

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

$$\sum_{k=1}^{n} a_{kj}\,\mathrm{cof}_{ki}(\mathbf{A}) = \delta_{ij} \det(\mathbf{A}),$$

όπου

$$\delta_{ij} = \begin{cases} 0_R, & \text{όταν } i \neq j, \\ 1_R, & \text{όταν } i = j. \end{cases}$$

(x) Για οιονδήποτε φυσικό αριθμό n ισχύουν οι ισότητες

$$\boxed{\det(\mathbf{A})\ \mathbf{I}_n = \mathbf{A}\cdot\mathbf{adj}(\mathbf{A}) = \mathbf{adj}(\mathbf{A})\cdot\mathbf{A}.} \tag{1.18}$$

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

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

Να αποδειχθεί ότι κάθε μέλος τής ακολουθίας διαδοχικώς εγκλειομένων συνόλων

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

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

1-18. 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

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

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

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

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

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

1-27. 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 $a \in R\setminus\{0_R\}$ είναι μη μηδενοδύναμο.

(ii) Εάν ο R είναι μια ακεραία περιοχή, τότε το μόνο ταυτοδύναμο στοιχείο $a \in R\setminus\{0_R\}$ 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 $\mathcal{C}([0,1]) := \left\{ f \in \mathbb{R}^{[0,1]} \mid f \text{ συνεχής} \right\}$ (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 (δηλαδή $\sqrt{|m|} \notin \mathbb{Q}$), να αποδειχθούν τα ακόλουθα:

(i) Για οιαδήποτε στοιχεία $a + b\sqrt{m}$ και $c + d\sqrt{m}$ τού δακτυλίου $\mathbb{Z}[\sqrt{m}]$ (βλ. (1.8)) 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. (1.8)) είναι *ακεραία περιοχή*.

(iii) Για κάθε $r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ (βλ. (1.9)) 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[19], 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

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

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.

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

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 $\varphi(\mathsf{X}) \in \mathbb{Z}_4[\mathsf{X}]$ 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 **απροσδιορίστου**) X με συντελεστές ειλημμένους από τον R.

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

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

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

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

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

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

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

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

(vii) Ένα στοιχείο $\varphi(\mathsf{X}) = \sum_{i=-n}^{\infty} a_i \mathsf{X}^i \in \mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!]$ με $a_{-n} \neq 0_R$ 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

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

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, 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 $|R^{\times}| \equiv 0 \pmod{2}$.

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 χαρ$(R) = m \in \mathbb{N}$ και 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 μκδ$(p, \text{ord}(a)) = 1$.

ΚΕΦΑΛΑΙΟ 2

Ιδεώδη και πηλικοδακτύλιοι

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

2.1 ΙΔΕΩΔΗ

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

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

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

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

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

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

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

2.1.3 Πρόταση. *Έστω $(R,+,\cdot)$ ένας δακτύλιος. Ένα μη κενό υποσύνολο I τού R είναι ένα αριστερό (και αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες εάν και μόνον εάν ισχύουν τα εξής:*
(i) $a-b\in I$, *για οιαδήποτε* $a,b\in I$.
(ii) $ra\in I$ *(και αντιστοίχως,* $ar\in I$ / $ra, ar\in I$*) για οιαδήποτε* $a\in I,\ r\in R$.

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

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

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

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

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

και

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

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

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

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

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

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

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

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

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

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

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

είναι ένα αριστερό και το σύνολο

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

ένα δεξιό ιδεώδες τού R.

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

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

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

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

και

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

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

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

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

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

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

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

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

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

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

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

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

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

πράγμα που έχουμε εκ των προτέρων αποκλείσει. □

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

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

(i) *Ο R είναι διαιρετικός δακτύλιος.*

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

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

ΑΠΟΔΕΙΞΗ. (i)⇔(ii) Εάν ο R είναι διαιρετικός δακτύλιος και I ένα αριστερό ιδεώδες αυτού με $\{0_R\} \subsetneqq I$, τότε υπάρχει κάποιο $a \in I \smallsetminus \{0_R\}$. Εξ ορισμού, το a διαθέτει αντίστροφο a^{-1}. Επειδή $1_R = a^{-1}a \in I$, έχουμε $I = R$. Και αντιστρόφως· υποθέτοντας ότι τα μόνα αριστερά ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R, και θεωρώντας οιοδήποτε στοιχείο $a \in R \setminus \{0_R\}$ και το αριστερό, μη τετριμμένο ιδεώδες Ra τού R, παρατηρούμε ότι

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

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

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

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

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

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

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

2.2 ΙΔΕΩΔΗ ΠΑΡΑΓΟΜΕΝΑ ΑΠΟ ΣΥΝΟΛΑ

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

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

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

των μελών τής οικογενείας όλων των ιδεωδών αυτού, τα οποία περιέχουν το A, είναι **το ιδεώδες το παραγόμενο από το** A ή το ιδεώδες **με γεννήτορες** τα στοιχεία τού A. Όταν $A = \varnothing$, τότε $\langle A \rangle = \{0_R\}$. Κάθε ιδεώδες τού R που μπορεί να γραφεί υπό τη μορφή $\langle A \rangle$, όπου $A \subseteq R$ είναι κάποιο πεπερασμένο υποσύνολο αυτού, ας πούμε το $A = \{a_1, \ldots, a_k\}$ (όπου $k \in \mathbb{N}$), καλείται **πεπερασμένως παραγόμενο**

ιδεώδες και συμβολίζεται απλούστερα ως $\langle a_1, \ldots, a_k \rangle$. Τέλος, κάθε ιδεώδες τού R που μπορεί γραφεί υπό τη μορφή $\langle a \rangle$, για κάποιο $a \in R$, καλείται **κύριο ιδεώδες** (έχον το a ως γεννήτορά του).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

και

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

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

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

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

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

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

και

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

οπότε

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

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

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

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

2.3 ΔΑΚΤΥΛΙΟΙ ΜΕ «ΛΙΓΑ» ΙΔΕΩΔΗ

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

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

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

2.3.2 Πρόταση. *Κάθε διαιρετικός δακτύλιος είναι απλός.*

ΑΠΟΔΕΙΞΗ. Άμεση συνέπεια τού πορίσματος 2.1.11. □

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

ΑΠΟΔΕΙΞΗ. Άμεση συνέπεια τού πορίσματος 2.1.9. □

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

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

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

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

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

απ' όπου έπεται ότι

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

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

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

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

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

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

σχηματίζεται η εξής ακολουθία διαδοχικώς εγκλειομένων κυρίων ιδεωδών:

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

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

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

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

2.4 ΛΟΓΙΣΜΟΣ ΜΕ ΙΔΕΩΔΗ

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

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

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

και

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

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

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

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

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

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

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

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

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

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

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

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

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

Επί παραδείγματι, εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων (πρβλ. 2.4.13 (iii)), έχουμε

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

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

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

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

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

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

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

όπου $Rab = \langle ab\rangle$. □

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

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

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

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

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

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

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

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

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

Επομένως, λόγω τής επιμεριστικής ιδιότητας,

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

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας,

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

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

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

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

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

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

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

Όμως, από τον ορισμό τού ιδεώδους,

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

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

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

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

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

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

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

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

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

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

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

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

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

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

(πρβλ. πόρισμα 2.4.13).

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

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

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

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

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

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

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

καλείται **μηδενοδύναμο ιδεώδες**.

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

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

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

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

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

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

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

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

Κατά το (iii) τής προτάσεως 2.2.2 υπάρχουν $r_1, \ldots, r_\kappa \in R$, τέτοια ώστε να ισχύει η ισότητα $x = \sum_{j=1}^{\kappa} r_j a_j$. Επειδή ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, έχουμε (λόγω τού ορισμού τού n, των ισοτήτων (2.2) και τού τύπου (1.6))

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

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

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

Ειδικότερα, για $m = \kappa n$ λαμβάνουμε

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

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

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

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

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

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

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

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

και αποτελεί ένα ιδεώδες τού R.

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

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

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

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

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

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

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

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

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

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

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

ήτοι $\langle m \rangle \cap \langle n \rangle \subseteq \langle \text{εκπ}(m,n) \rangle$. Και αντιστρόφως· εάν $a \in \langle \text{εκπ}(m,n) \rangle$, τότε έχουμε $a = \mu\, \text{εκπ}(m,n)$, για κάποιον $\mu \in \mathbb{Z}$, οπότε[6]

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

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

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

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

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

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

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

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

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

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

για κάποιον $c \in \mathbb{Z}$. Άρα

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

οπότε $rI_2 + rI_3 = r\,(I_2 + I_3) \subseteq I_1 + I_1 = I_1 \Longrightarrow r \in I_1 : (I_2 + I_3)$. Εν συνεχεία, υποθέτουμε ότι $r \in (I_1 \cap I_2) : I_3$, ήτοι ότι ισχύει $rI_3 \subseteq I_1 \cap I_2$. Επειδή $I_1 \cap I_2 \subseteq I_1$ και $I_1 \cap I_2 \subseteq I_2$, έχουμε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, δηλαδή $r \in (I_1 : I_3) \cap (I_2 : I_3)$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) \cap (I_2 : I_3)$, τότε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, οπότε $rI_3 \subseteq I_1 \cap I_2 \Longrightarrow r \in (I_1 \cap I_2) : I_3$.
(iii) Έστω τυχόν $r \in (I_1 : I_2)\ I_2$. Τότε

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

οπότε

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

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

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

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

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

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

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

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

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

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

οπότε όντως $J_1 = J_2$. □

2.5 ΠΡΩΤΑ ΚΑΙ ΜΕΓΙΣΤΙΚΑ ΙΔΕΩΔΗ

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

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

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

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

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

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

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

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

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

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

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

(iii) Το

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

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

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

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

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

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

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

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

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

2.5.5 Παρατήρηση. Ως γνωστόν, η τομή δυο ιδεωδών ενός δακτυλίου είναι ιδεώδες αυτού (βλ. πρόταση 2.1.5). Ωστόσο, η τομή δυο πρώτων ιδεωδών δεν είναι κατ' ανάγκην πρώτο ιδεώδες. Επί παραδείγματι, σύμφωνα με την πρόταση 2.5 .4 και το (i) τού πορίσματος 2.4.13, τα ιδεώδη $\langle 3\rangle$ και $\langle 5\rangle$ είναι πρώτα ιδεώδη τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών αλλά η τομή τους $\langle 3\rangle \cap \langle 5\rangle = \langle 15\rangle$ δεν είναι πρώτο ιδεώδες. (Πρβλ. με το (i) τής ασκήσεως **2-32**.)

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

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

2.5.7 Παραδείγματα. (i) Το ιδεώδες $\mathfrak{m} := \{(x, 2y) \mid x, y \in \mathbb{Z}\}$ τού δακτυλίου $\mathbb{Z}\times\mathbb{Z}$ είναι μεγιστικό. Πράγματι· εάν το $\mathfrak{n}$ είναι ένα ιδεώδες τού $\mathbb{Z}\times\mathbb{Z}$, για το οποίο ισχύει $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq \mathbb{Z}\times\mathbb{Z}$, τότε υπάρχει κάποιο στοιχείο τής μορφής $(a, 2b+1)$ εντός τού $\mathfrak{n}$, όπου a, b κατάλληλοι ακέραιοι αριθμοί. Επομένως,

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

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

(ii) Το ιδεώδες

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

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

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathfrak{n} \smallsetminus \mathfrak{m}, \text{ με } a, b \in \mathbb{R}, \ \ d \in \mathbb{R} \smallsetminus \{0\}.$$

Επομένως,

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

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

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

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

Πρώτη περίπτωση: Εάν $a \equiv 1 (\bmod 3)$ και $b \equiv 0 (\bmod 3)$, τότε

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

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

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

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

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

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

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

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

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

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

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

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

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

και

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ή η ακόλουθη ασυνήθης:

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

διάταξη των ακεραίων, αποτελεί ένα ολικώς διατεταγμένο σύνολο.

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

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

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

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

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

(i) Ένα στοιχείο $x \in A$ καλείται **άνω φράγμα** τού B (εντός τού A) ως προς την “$\preceq$” όταν $y \preceq x, \ \forall y \in B$.

(ii) Ένα στοιχείο $x \in A$ καλείται **κάτω φράγμα** τού B (εντός τού A) ως προς την “$\preceq$” όταν $x \preceq y, \ \forall y \in B$.

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

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

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

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

2.5.15 Ορισμός. Ένα μερικώς διατεταγμένο σύνολο $(A, \preceq)$ λέγεται **επαγωγικώς διατεταγμένο** όταν κάθε ολικώς διατεταγμένο[7] υποσύνολό του (ως προς την "$\preceq$") διαθέτει ένα άνω φράγμα (εντός τού A).

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

(ii) Το $(\mathfrak{P}(A), \subseteq))$, όπου A ένα μη κενό σύνολο, δεν είναι κατ' ανάγκην επαγωγικώς διατεταγμένο. Ωστόσο, κάθε υποσύνολο τού $\mathfrak{P}(A)$ τής μορφής $\{B_1, B_2, B_3, ...\}$, όπου $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$, είναι επαγωγικώς διατεταγμένο[8] (ως προς την "$\subseteq$").

Το ακόλουθο *λήμμα τού Zorn*[9] εφαρμόζεται σε μια πληθώρα αποδείξεων θεωρημάτων σχετιζομένων με την ύπαρξη μεγιστικών στοιχείων (ως προς δεδομένες σχέσεις διατάξεως):

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

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

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

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

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

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

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

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

[8] Σημειωτέον ότι *το ίδιο το* $\{B_1, B_2, B_3, \ldots\}$ έχει το $\bigcup_{k \in \mathbb{N}} B_k \in \mathfrak{P}(A)$ ως άνω φράγμα του.

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

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

ΑΠΟΔΕΙΞΗ. Έστω $I \subsetneqq R$ ένα ιδεώδες τού R και έστω[10]

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

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

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

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

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

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

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

Συνεπώς,

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

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

2.5.21 Παρατήρηση. (i) Το θεώρημα 2.5.20 παραμένει εν ισχύ ακόμη και εάν κανείς αντικαταστήσει τα (αμφίπλευρα) μεγιστικά ιδεώδη (τής διατυπώσεως και τής

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

αποδείξεώς του) με αριστερά μεγιστικά ιδεώδη (και αντιστοίχως, με δεξιά μεγιστικά ιδεώδη) χρησιμοποιώντας τά προαναφερθέντα στο εδάφιο 2.5.19 (ii).

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

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

Είναι άμεσος ο έλεγχος τού ότι η τριάδα $(\mathbb{Q},+,\star)$ αποτελεί έναν δακτύλιο. Επιπροσθέτως, κάθε υποομάδα τής $(\mathbb{Q},+)$ αποτελεί ένα ιδεώδες τού $(\mathbb{Q},+,\star)$. Αρκεί λοιπόν να αποδειχθεί ότι η $(\mathbb{Q},+)$ *στερείται μεγιστικών υποομάδων*[11] (αφού οιοδήποτε μεγιστικό ιδεώδες τού $(\mathbb{Q},+,\star)$ θα όφειλε να είναι μεγιστική υποομάδα τής $(\mathbb{Q},+)$). Ας υποθέσουμε ότι η $(\mathbb{Q},+)$ διαθέτει κάποια μεγιστική υποομάδα $H\subsetneqq\mathbb{Q}$ και ότι $\frac{r}{s}\in\mathbb{Q}\smallsetminus H$, για κάποιους $r,s\in\mathbb{Z}\smallsetminus\{0\}$. Τότε

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

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

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

Επειδή

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.6 ΠΗΛΙΚΟΔΑΚΤΥΛΙΟΙ

Έστω $(R, +, \cdot)$ ένας δακτύλιος και έστω I ένα ιδεώδες του. Επειδή η προσθετική ομάδα $(R, +)$ είναι αβελιανή, το ζεύγος $\left(I, +|_{I \times I}\right)$ αποτελεί μια ορθόθετη προσθετική υποομάδα της. Επομένως υπάρχει μια καλώς ορισμένη ομάδα πηλίκων R/I με πρόσθεση[12]:

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

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

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

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

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

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

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

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

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

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

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

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

και

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

για οιαδήποτε $a, b, c \in R$. □

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) Εάν $a \in R$, τότε

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

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

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

οπότε και αυτή η αμφίπλευρη συνεπαγωγή είναι αληθής. □

2.6.4 Θεώρημα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και το $\mathfrak{p}$ ένα ιδεώδες τού R, τότε τα ακόλουθα είναι ισοδύναμα:*
(i) $\mathfrak{p} \subsetneqq R$ *και το $\mathfrak{p}$ είναι πρώτο ιδεώδες τού R.*
(ii) *Ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι μεταθετικός με το $0_R + \mathfrak{p}$ ως μηδενικό και το $1_R + \mathfrak{p}$ ως μοναδιαίο του στοιχείο.
(i)⇒(ii): Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού R, τότε $1_R + \mathfrak{p} \neq \mathfrak{p}$ αφού $\mathfrak{p} \subsetneqq R$. Για οιαδήποτε $a, b \in R$, για τα οποία ισχύει η ισότητα $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$, έχουμε

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) Εάν ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι διαιρετικός δακτύλιος, παρατηρούμε εν πρώτοις ότι $1_R+\mathfrak{m} \neq 0_R+\mathfrak{m} \Longrightarrow 1_R \notin \mathfrak{m} \Longrightarrow \mathfrak{m} \subsetneqq R$. Εν συνεχεία, υποθέτουμε ότι το $\mathfrak{n}$ είναι ένα ιδεώδες τού R με $\mathfrak{m} \subsetneqq \mathfrak{n} \subseteq R$. Έστω τυχόν $a \in \mathfrak{n}\smallsetminus\mathfrak{m}$. Το $a+\mathfrak{m}$ έχει (εξ υποθέσεως) πολλαπλασιαστικό αντίστροφο, ας το πούμε $b+\mathfrak{m}$, εντός τού $R/\mathfrak{m}$. Συνεπώς,

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

και

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

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

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

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

$\boxed{2.7}$ ΤΟΠΙΚΟΙ ΔΑΚΤΥΛΙΟΙ

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

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

Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:

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

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

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

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

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Θεωρούμε τυχόντα στοιχεία $a \in \mathfrak{m}_R$ και $r \in R$. Αρκεί να αποδείξουμε ότι $ra \in \mathfrak{m}_R$. Εάν είχαμε $ra \notin \mathfrak{m}_R$, τότε $ra \in R^{\times}$, οπότε θα υπήρχε $b \in R$ με $(ra)b = a(rb) = 1_R$. Τούτο θα σήμαινε ότι $a \in R^{\times}$. Άτοπο! Άρα $ra \in \mathfrak{m}_R$.

(ii)⇒(iii): Λόγω τού (ii) τού πορίσματος 2.6.5 αρκεί προς τούτο να δειχθεί ότι ο πηλικοδακτύλιος $R/\mathfrak{m}_R$ είναι σώμα. Μάλιστα, επειδή

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

είναι αρκετό να δειχθεί ότι $r + \mathfrak{m}_R \in (R/\mathfrak{m}_R)^{\times}$ για κάθε $r \in R^{\times}$. Τούτο έπεται από το (iii) τής προτάσεως 2.6.3.

(iii)⇒(iv): Έστω τυχόν στοιχείο $a \in R$. Εάν ίσχυε $a \in \mathfrak{m}_R$ και $1_R - a \in \mathfrak{m}_R$, τότε θα καταλήγαμε στην αντίφαση: $a + (1_R - a) = 1_R \in \mathfrak{m}_R \Longrightarrow \mathfrak{m}_R = R$.

(iv)⇒(i): Ας υποθέσουμε ότι υπάρχουν $a, b \in \mathfrak{m}_R$ με $a - b \notin \mathfrak{m}_R$. Τότε $a - b \in R^{\times}$, οπότε $\exists c \in R : (a-b)\,c = ac + (-bc) = 1_R$. Εξ υποθέσεως, είτε $ac \in R^{\times}$ είτε $-bc \in R^{\times}$. Εάν $ac \in R^{\times}$, τότε

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

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

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

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

(ii) Ο δακτύλιος

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

των p-αδικών κλασμάτων (όπου p πρώτος, βλ. άσκηση **1-11**, σελ. 34) είναι τοπικός δακτύλιος, καθότι το (κύριο) ιδεώδες

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ασκήσεις

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2-4. Έστω

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

και έστω

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

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

2-5. Εάν η $(I_n)_{n \in \mathbb{N}}$ είναι μια ακολουθία (αριστερών/δεξιών/αμφιπλεύρων) ιδεωδών ενός δακτυλίου R με

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

να αποδειχθεί ότι η ένωση $I := \bigcup_{j=1}^{\infty} I_j$ των μελών αυτής αποτελεί ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R.

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

2-7. Να αποδειχθεί ότι το σύνολο

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

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

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

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

και

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

να αποδειχθούν τα ακόλουθα:

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

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

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

(iv) Το J_p δεν είναι κύριο ιδεώδες.

2-9. Να αποδειχθούν τα ακόλουθα:

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

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

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

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

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

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

όπου

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) Οι απεικονίσεις

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

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

και

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

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

(v) Οι απεικονίσεις Φ_{α} και Φ_{δ} δεν είναι κατ' ανάγκην επιρριπτικές (ακόμη και όταν ο R έχει μοναδιαίο στοιχείο).

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

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

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

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

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

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

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

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

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

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

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

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

(iii) Το $\mathrm{SLT}_n(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{LT}_n(R)$.

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

(v) Εάν ο R έχει μοναδιαίο στοιχείο, τότε

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

και, κατ' αναλογίαν,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(vii) $\mathrm{Rad}(I)\, \mathrm{Rad}(J) \subseteq \mathrm{Rad}(I\, J) = \mathrm{Rad}(\mathrm{Rad}(I)\, \mathrm{Rad}(J))$,

(viii) $\mathrm{Rad}(I)\; : \mathrm{Rad}(J) \supseteq \mathrm{Rad}(I\; : J)$.

(ix) $I = \mathrm{Rad}(I) \Longleftrightarrow \mathrm{Nil}(R/I) = \{0_{R/I}\}\; (= \{I\})$.

2-24. Έστω $m \in \mathbb{N}$, $m \geq 2$. Εάν $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $k \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, είναι η παράσταση τού m ως γινομένου κατάλληλων δυνάμεων διακεκριμένων πρώτων αριθμών $p_1, \ldots, p_k$, να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Nil}(\mathbb{Z}_m) = \{[0]_m\} \Leftrightarrow \alpha_1 = \cdots = \alpha_k = 1$.

(ii) Το ριζικό τού κυρίου ιδεώδους $\langle m \rangle$ τού δακτυλίου $\mathbb{Z}$ των ακεραίων ισούται με

$$\mathrm{Rad}\,(\langle m \rangle) = \mathrm{Rad}\,(\langle -m \rangle) = \langle p_1 \cdots p_k \rangle\, .$$

2-25. Εάν το I είναι ένα ιδεώδες ενός δακτυλίου R, να αποδειχθούν τα ακόλουθα:

(i) Ο πηλικοδακτύλιος R/I είναι μεταθετικός εάν και μόνον εάν $ab - ba \in I$ για οιαδήποτε $a, b \in R$.

(ii) Ο πηλικοδακτύλιος R/I έχει μοναδιαίο στοιχείο εάν και μόνον εάν υπάρχει κάποιο στοιχείο $e \in R$, τέτοιο ώστε να ισχύει

$$ae - a \in I \ \text{ και } \ ea - a \in I, \quad \forall a \in R.$$

2-26. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Να αποδειχθεί ότι τα ακόλουθα είναι ισοδύναμα:

(i) Ο R είναι ακεραία περιοχή.

(ii) Το τετριμμένο ιδεώδες $\{0_R\}$ τού R είναι πρώτο ιδεώδες.

2-27. Να αποδειχθεί ότι το κύριο ιδεώδες $\langle (\mathsf{X}-1)(\mathsf{X}-2) \rangle$ τού $\mathbb{Q}[\mathsf{X}]$ δεν είναι πρώτο ιδεώδες.

2-28. Να αποδειχθεί ότι ο πηλικοδακτύλιος $\mathbb{Z}_2[\mathsf{X}]/\left\langle \mathsf{X}^2+1 \right\rangle$ δεν είναι ακεραία περιοχή. (Ως εκ τούτου, το κύριο ιδεώδες $\left\langle \mathsf{X}^2+1 \right\rangle$ τής ακεραίας περιοχής $\mathbb{Z}_2[\mathsf{X}]$ δεν είναι πρώτο. Βλ. θεώρημα 2.6.4.)

2-29. Να αποδειχθεί ότι οι έννοιες *πρώτο* και *μεγιστικό* ιδεώδες οιουδήποτε *πεπερασμένου* μεταθετικού δακτυλίου με μοναδιαίο στοιχείο ταυτίζονται.

2-30. Έστω R ένας δακτύλιος τού Boole (βλ. άσκηση **1-4**). Να αποδειχθούν τα εξής:

(i) Κάθε πεπερασμένως παραγόμενο ιδεώδες τού R είναι κύριο ιδεώδες.

(ii) Έστω I ένα μη τετριμμένο γνήσιο ιδεώδες τού R. Τότε το I είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.

2-31. Έστω M ένα μη κενό σύνολο και έστω $(\mathfrak{P}(M), \triangle, \cap)$ ο δακτύλιος Boole ο ορισθείς στην άσκηση **1-7**. Να αποδειχθούν τα εξής:

(i) Κάθε πεπερασμένως παραγόμενο ιδεώδες τού $\mathfrak{P}(M)$ είναι κύριο.

(ii) Κάθε κύριο ιδεώδες τού δακτυλίου $\mathfrak{P}(M)$ γράφεται υπό τη μορφή $\mathfrak{P}(M')$, όπου $\varnothing \neq M' \subseteq M$.

(iii) Το $\mathfrak{P}(M \setminus \{x\})$ είναι μεγιστικό ιδεώδες τού $\mathfrak{P}(M)$ για κάθε $x \in M$.

2-32. Έστω R ένας μεταθετικός δακτύλιος. Να αποδειχθούν τα εξής:

(i) Εάν τα $\mathfrak{p}_1$ και $\mathfrak{p}_2$ είναι δυο πρώτα ιδεώδη τού R, τότε η τομή $\mathfrak{p}_1 \cap \mathfrak{p}_2$ είναι πρώτο ιδεώδες τού $R \Longleftrightarrow$ είτε $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ είτε $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$.

(ii) Εάν η $(\mathfrak{p}_n)_{n \in \mathbb{N}}$ είναι μια ακολουθία πρώτων ιδεωδών τού R με

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \subseteq \mathfrak{p}_{n+1} \subseteq \cdots,$$

τότε η ένωση $\bigcup\limits_{j=1}^{\infty} \mathfrak{p}_j$ των μελών της αποτελεί ένα πρώτο ιδεώδες τού R.

(iii) Εάν η $(\mathfrak{p}_n)_{n\in\mathbb{N}}$ είναι μια ακολουθία πρώτων ιδεωδών τού R με

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n \supseteq \mathfrak{p}_{n+1} \supseteq \cdots ,$$

τότε η τομή $\bigcap_{j=1}^{\infty} \mathfrak{p}_j$ των μελών της αποτελεί ένα πρώτο ιδεώδες τού R.

2-33. Έστω R ένας μεταθετικός δακτύλιος και έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες αυτού. Εάν $n \in \mathbb{N}$ και εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη τού R, να αποδειχθούν οι ακόλουθες συνεπαγωγές:

(i) $I_1 \cdots I_n \subseteq \mathfrak{p} \Longleftrightarrow \exists\, j \in \{1, \ldots, n\} : I_j \subseteq \mathfrak{p}$.

(ii) $\mathfrak{p} = I_1 \cap \cdots \cap I_n \Longrightarrow \exists\, j \in \{1, \ldots, n\} : \mathfrak{p} = I_j$.

2-34. Έστω R ένας μεταθετικός δακτύλιος και έστω I ένα ιδεώδες αυτού. Εάν τα $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, $n \in \mathbb{N}$, είναι πρώτα ιδεώδη τού R, τέτοια ώστε $I \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, να αποδειχθεί ότι $\exists\, j \in \{1, \ldots, n\} : I \subseteq \mathfrak{p}_j$.

2-35. Έστω R ένας δακτύλιος. Εάν τα $\mathfrak{m}_1, \mathfrak{m}_2$ είναι δυο μεγιστικά ιδεώδη τού R και $\mathfrak{m}_1 \neq \mathfrak{m}_2$, να αποδειχθούν τα εξής:

(i) $\mathfrak{m}_1 + \mathfrak{m}_2 = R$.

(ii) Εάν ο R είναι μεταθετικός με μοναδιαίο στοιχείο, τότε $\mathfrak{m}_1\mathfrak{m}_2 = \mathfrak{m}_1 \cap \mathfrak{m}_2$.

2-36. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ως **πρώτο φάσμα τού** R ορίζεται το σύνολο όλων των πρώτων ιδεωδών τού R, συμβολιζόμενο ως $\mathrm{Spec}(R)$. Για κάθε ιδεώδες I τού R εισάγουμε τον συμβολισμό:

$$\boxed{\mathbf{V}(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}.}$$

Να αποδειχθούν τα ακόλουθα:

(i) $\mathrm{Spec}(R) = \varnothing \Longleftrightarrow$ ο R είναι τετριμμένος δακτύλιος.

(ii) Εάν τα I, J είναι δυο ιδεώδη τού R, τότε $I \subseteq J \Longrightarrow \mathbf{V}(I) \supseteq \mathbf{V}(J)$.

(iii) $\mathbf{V}(I) = \varnothing \Longleftrightarrow I = R$.

(iv) $\mathbf{V}(\{0_R\}) = \mathrm{Spec}(R)$.

(v) Εάν $n \in \mathbb{N}$ και εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη τού R, τότε

$$\mathbf{V}(I_1) \cup \cdots \cup \mathbf{V}(I_n) = \mathbf{V}(I_1 \cdots I_n) = \mathbf{V}(I_1 \cap \cdots \cap I_n).$$

(vi) Εάν η $\{I_\lambda\}_{\lambda\in\Lambda}$ είναι μια οικογένεια ιδεωδών τού R, τότε

$$\bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda) = \mathbf{V}\left(\left\langle \bigcup_{\lambda\in\Lambda} I_\lambda \right\rangle\right).$$

[*Σημείωση*: Είναι πρόδηλο εκ των ανωτέρω ότι το $\mathrm{Spec}(R)$ εφοδιάζεται με μία *τοπολογία* έχουσα τα μέλη τής οικογενείας $\{\mathbf{V}(I) \mid I$ ιδεώδες τού $R\}$ ως *κλειστά σύνολα*. Η εν λόγω τοπολογία καλείται **τοπολογία Zariski** επί τού $\mathrm{Spec}(R)$ και διαδραματίζει σημαντικό ρόλο στη Μεταθετική Άλγεβρα και στην Αλγεβρική Γεωμετρία.]

2-37. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα υποσύνολο $\varnothing \neq \mathsf{S} \subseteq R$ καλείται **πολλαπλασιαστικώς κλειστό σύνολο** όταν $1_R \in \mathsf{S}$ και $ab \in \mathsf{S}$ για οιαδήποτε $a, b \in \mathsf{S}$. Να αποδειχθούν τα ακόλουθα:

(i) Εάν το $\mathsf{S} \subseteq R$ είναι ένα πολλαπλασιαστικώς κλειστό σύνολο και το I ένα ιδεώδες τού R με $I \cap \mathsf{S} = \varnothing$, τότε

$$\exists \mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq I \text{ και } \mathfrak{p} \cap \mathsf{S} = \varnothing.$$

[*Υπόδειξη*: Να επαληθευθεί ότι το

$$(\{J \mid J \text{ ιδεώδες τού } R \text{ με } J \supseteq I \text{ και } J \cap \mathsf{S} = \varnothing\}, \subseteq)$$

είναι επαγωγικώς διατεταγμένο και να εφαρμοσθεί το λήμμα 2.5.17 τού Zorn.]

(ii) Για κάθε ιδεώδες I τού R ισχύει η ισότητα

$$\mathrm{Rad}\,(I) = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathbf{V}(I)\}.$$

Σημειωτέον ότι για $I = \{0_R\}$,

$$\mathrm{Nil}\,(R) = \mathrm{Rad}\,(\{0_R\}) = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(R)\}.$$

[*Υπόδειξη*: Για την απόδειξη τού αντίστροφου εγκλεισμού "$\supseteq$" να υποτεθεί ότι υπάρχει στοιχείο $a \in \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathbf{V}(I)\}$ με $a \notin \mathrm{Rad}(I)$ και να εφαρμοσθεί το (i) για το πολλαπλασιαστικώς κλειστό σύνολο $\mathsf{S} := \{a^n \mid n \in \mathbb{N}_0\}$, ούτως ώστε να προκύψει αντίφαση.]

2-38. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν τα I, J είναι ιδεώδη τού R, να αποδειχθούν τα ακόλουθα:

(i) $\mathbf{V}(I) \subseteq \mathbf{V}(J) \Longleftrightarrow \mathrm{Rad}(J) \supseteq \mathrm{Rad}(I)$.

(ii) $\mathbf{V}(I) = \mathbf{V}(J) \Longleftrightarrow \mathrm{Rad}(I) = \mathrm{Rad}(J)$.

(iii) $\mathbf{V}(I) = \mathrm{Spec}(R) \Longleftrightarrow I \subseteq \mathrm{Nil}(R)$.

2-39. Να αποδειχθεί ότι τα μόνα ταυτοδύναμα στοιχεία ενός τοπικού δακτυλίου R είναι τα 0_R και 1_R.

2-40. Έστω $m \in \mathbb{N}$, $m \geq 2$. Να αποδειχθεί ότι ο δακτύλιος $\mathbb{Z}_m$ (ο ορισθείς στο εδάφιο 1.1.4 (iv)) είναι τοπικός εάν και μόνον εάν $m = p^\nu$, όπου p κάποιος πρώτος αριθμός και $\nu \in \mathbb{N}$.

ΚΕΦΑΛΑΙΟ 3

Ομομορφισμοί δακτυλίων

Οι απεικονίσεις μεταξύ δυο δακτυλίων, οι οποίες τυγχάνει να μεταφέρουν τις εκάστοτε θεωρούμενες πράξεις προσθέσεως και πολλαπλασιασμού κατά τρόπο συμβατό, καλούνται *ομομορφισμοί δακτυλίων*. Οι *εμφυτεύσεις* δακτυλίων εντός άλλων διασφαλίζονται μέσω κατασκευής *μονομορφισμών*, ήτοι ενριπτικών ομομορφισμών. Οι *πυρήνες* των ομομορφισμών δακτυλίων αποτελούν ιδεώδη και κάθε ιδεώδες ενός δακτυλίου μπορεί να ιδωθεί ως πυρήνας τού λεγομένου *φυσικού επιμορφισμού*. Το *θεώρημα αντιστοιχίσεως* περιγράφει τον τρόπο συσχετισμού των ιδεωδών ενός δακτυλίου με τα ιδεώδη τής εικόνας αυτού μέσω ενός επιμορφισμού. Τέλος, τα *θεωρήματα ισομορφισμών* μάς παρέχουν χρήσιμες πληροφορίες για τις περιπτώσεις «ταυτίσεως» ορισμένων χαρακτηριστικών δακτυλίων και πηλικοδακτυλίων, κατ' αναλογίαν προς ό,τι συμβαίνει με τα συνώνυμα θεωρήματα περί ομάδων.

3.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

3.1.1 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι και $f : R \longrightarrow R'$ μια απεικόνιση, τότε η f καλείται **ομομορφισμός (δακτυλίων)** όταν ισχύουν οι ισότητες[1]

$$\boxed{f(a+b) = f(a) + f(b)} \quad \text{και} \quad \boxed{f(ab) = f(a)\,f(b)} \tag{3.1}$$

για όλα τα $a, b \in R$.

[1]Προσοχή! Παρά το γεγονός ότι χρησιμοποιούμε *ίδιο συμβολισμό* για τις πράξεις επί των R και R', αυτές ενδέχεται να είναι *διαφορετικές*!

Ένας ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ ονομάζεται

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιρριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιρριπτική,
ενδομορφισμός (τού R**)**	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$R = R'$,
αυτομορφισμός (τού R**)**	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η f είναι αμφιρριπτικός ενδομορφισμός.

(Φυσικά, αυτές οι έννοιες εμπεριέχουν τις αντίστοιχες έννοιες για τις επί μέρους δομές, δηλαδή εκείνες των εκάστοτε μετεχουσών αβελιανών προσθετικών ομάδων και πολλαπλασιαστικών ημιομάδων).

3.1.2 Παραδείγματα. (i) Έστω m ένας φυσικός αριθμός. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \quad n \longmapsto [n]_m \,.$$

Είναι εύκολο να αποδειχθεί ότι η f είναι ένας επιμορφισμός δακτυλίων.

(ii) Η απεικόνιση $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f(n) := 2n$ *δεν είναι* ομομορφισμός δακτυλίων, παρότι *είναι* ισομορφισμός μεταξύ των αντιστοίχων προσθετικών ομάδων!

(iii) Έστω $(2\,\mathbb{Z}, +, \star)$ ο δακτύλιος ο αποτελούμενος από τους αρτίους ακεραίους με τη συνήθη πρόσθεση και τον ακόλουθο «τροποποιημένο» πολλαπλασιασμό:

$$m \star n := \frac{m \cdot n}{2} \,.$$

Τότε η $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f(n) := 2n$ (όπως και στο (ii)) αποτελεί *ισομορφισμό δακτυλίων*.

(iv) Εάν το K είναι ένα σώμα με χαρ$(K) = p > 0$, τότε η απεικόνιση

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

είναι ένας ενδομορφισμός (πρβλ. πρόταση 1.4.8 (i)) και καλείται, ιδιαιτέρως, **απεικόνιση τού Frobenius**.

(v) Ο ομομορφισμός

$$\mathbb{C} \longrightarrow \mathbb{C}, \;\; z = a + ib \longmapsto a - ib = \overline{z},$$

είναι ένας αυτομορφισμός τού σώματος των μιγαδικών αριθμών.

(vi) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \subsetneqq \mathbb{C}$$

το αριθμητικό τετραγωνικό σώμα το αντιστοιχιζόμενο στον m (βλ. άσκηση **1-37**). Τότε η απεικόνιση

$$f : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}(\sqrt{m}), \quad f(a + b\sqrt{m}) := a - b\sqrt{m},$$

αποτελεί έναν αυτομορφισμό τού $\mathbb{Q}(\sqrt{m})$ (βλ. άσκηση **3-5**).

(vii) Η *μηδενική απεικόνιση* $f : R \longrightarrow S$ μεταξύ δυο δακτυλίων R και S, όπου $f(a) = 0_S$ για κάθε $a \in R$, είναι ένας ομομορφισμός δακτυλίων (ο λεγόμενος **μηδενικός ομομορφισμός**). Σημειωτέον ότι όταν κανείς εκ των R, S δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιρριπτικός.

(viii) Εάν $f : R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων και

$$\mathrm{in}_{\mathrm{Im}(f),S} : \mathrm{Im}(f) \longrightarrow S, \ s \longmapsto \mathrm{in}_{\mathrm{Im}(f),S}(s) := s,$$

η συνήθης ένθεση τής εικόνας του εντός τού S, τότε $f = \mathrm{in}_{\mathrm{Im}(f),S} \circ \check{f}$, όπου

$$\boxed{\check{f} : R \longrightarrow \mathrm{Im}(f), \ r \longmapsto \check{f}(r) := f(r),}$$

ο επιμορφισμός ο επαγόμενος μέσω τού f.

3.1.3 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Εάν $n \in \mathbb{N}$ και εάν τα $a_1, ..., a_n$ είναι στοιχεία τού R, τότε*

$$f(\sum_{j=1}^{n} a_j) = \sum_{j=1}^{n} f(a_j) \qquad \textit{και} \qquad f(\prod_{j=1}^{n} a_j) = \prod_{j=1}^{n} f(a_j).$$

ΑΠΟΔΕΙΞΗ. Έπεται κατόπιν χρήσεως των ισοτήτων (3.1) και μαθηματικής επαγωγής ως προς τον n. □

3.1.4 Πρόταση. *Ένας ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ έχει τις εξής ιδιότητες:*

(i) $f(0_R) = 0_{R'}$ *και* $f(-a) = -f(a), \forall a \in R$.

(ii) *Για κάθε $a \in R$ ισχύουν οι ισότητες:*

$$f(na) = n f(a), \ \forall n \in \mathbb{Z}, \ \textit{και} \ \ f(a^n) = f(a)^n, \ \forall n \in \mathbb{N}.$$

(iii) *Εάν ο S είναι ένας υποδακτύλιος τού R, τότε η εικόνα του $f(S)$ μέσω τής f είναι ένας υποδακτύλιος τού R'.*

(iv) *Εάν ο* S' *είναι ένας υποδακτύλιος τού* R', *τότε η αντίστροφή του εικόνα* $f^{-1}(S')$ *μέσω τής* f *είναι ένας υποδακτύλιος τού* R.

(v) *Εάν ο* R *είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε και ο* $f(R)$ *είναι δακτύλιος με μοναδιαίο στοιχείο, και μάλιστα ισχύει η ισότητα* $f(1_R) = 1_{f(R)}$.

(vi) *Εάν ο* R *είναι ένας δακτύλιος με μοναδιαίο στοιχείο, η* f *μη μηδενικός ομομορφισμός και ο* R' *διαιρετικός δακτύλιος ή ακεραία περιοχή, τότε* $f(1_R) = 1_{R'}$.

(vii) *Εάν ο* R *είναι ένας μεταθετικός δακτύλιος, τότε και ο* $f(R)$ *είναι μεταθετικός.*

(viii) *Εάν ο* R *είναι ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και η* f *μη μηδενικός ομομορφισμός, τότε*

$$f(a^{-1}) \in f(R)^{\times}, \ f(a^{-1}) = [f(a)]^{-1}, \ \forall a \in R^{\times},$$

και, γενικότερα,

$$f(a^n) = f(a)^n, \ \forall a \in R^{\times} \textit{ και } \forall n \in \mathbb{Z}.$$

(ix) *Εάν η* f *είναι μονομορφισμός και ο* R *ακεραία περιοχή (και αντιστοίχως, στρεβλό σώμα/σώμα), τότε και ο* $f(R)$ *είναι ακεραία περιοχή (και αντιστοίχως, στρεβλό σώμα/σώμα).*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, οπότε ισχύει η ισότητα $f(0_R) = 0_{R'}$. Εξάλλου, για κάθε $a \in R$, έχουμε

$$0_{R'} = f(0_R) = f(a + (-a)) = f(a) + f(-a) \Longrightarrow f(-a) = -f(a).$$

(ii) Η απόδειξη έπεται από την πρόταση 3.1.3 και τη δεύτερη ισότητα τού (i).

(iii) Εάν $b_1, b_2 \in f(S)$, τότε υπάρχουν $a_1, a_2 \in S$, τέτοια ώστε $f(a_1) = b_1$ και $f(a_2) = b_2$. Επειδή ο S είναι ένας υποδακτύλιος τού R,

$$\left.\begin{array}{r} a_1 - a_2 \in S, \\ a_1 a_2 \in S \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in f(S), \\ b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(S), \end{array}\right.$$

οπότε η εικόνα $f(S)$ τού S μέσω τής f είναι όντως ένας υποδακτύλιος τού R'.

(iv) Εάν $a_1, a_2 \in f^{-1}(S')$, τότε $f(a_1) \in S'$ και $f(a_2) \in S'$. Κι επειδή ο S' είναι υποδακτύλιος τού R',

$$\left.\begin{array}{r} f(a_1 - a_2) = f(a_1) - f(a_2) \in S', \\ f(a_1 a_2) = f(a_1) f(a_2) \in S' \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a_1 - a_2 \in f^{-1}(S'), \\ a_1 a_2 \in f^{-1}(S'), \end{array}\right.$$

ήτοι *και* η αντίστροφή του εικόνα $f^{-1}(S')$ μέσω τής f είναι ένας υποδακτύλιος τού δακτυλίου R.

(v) Έστω b τυχόν στοιχείο τού $f(R)$. Τότε υπάρχει ένα $a \in R$, τέτοιο ώστε να ισχύει η ισότητα $f(a) = b$. Άρα

$$f(1_R)f(a) = f(1_R a) = f(a), \quad f(a)f(1_R) = f(a1_R) = f(a),$$

οπότε ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο και $f(1_R) = 1_{f(R)}$.

(vi) Επειδή -εξ υποθέσεως- ο f δεν είναι ο μηδενικός ομομορφισμός, θα υπάρχει ένα $a \in R$, τέτοιο ώστε $f(a) \neq 0_{R'}$. Εξ αυτού έπεται ότι

$$f(a) \cdot 1_{R'} = f(a) = f(a \cdot 1_R) = f(a)f(1_R) \Longrightarrow f(a)\left(f\left(1_R\right) - 1_{R'}\right) = 0_{R'}.$$

Εάν ο R' είναι διαιρετικός δακτύλιος, τότε υπάρχει το αντίστροφο $f(a)^{-1}$ τού $f(a)$, με το οποίο μπορούμε να πολλαπλασιάσουμε αμφότερα τα μέλη τής ανωτέρω ισότητας και να λάβουμε $f(1_R) = 1_{R'}$. Εάν, από την άλλη μεριά, ο R' είναι ακεραία περιοχή, τότε μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα κάνοντας χρήση τού νόμου τής διαγραφής 1.2.5.

(vii) Προφανώς, για κάθε $a, b \in R$, έχουμε

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

(viii) Για κάθε $a \in R^\times$ έχουμε

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_R) = f(a^{-1}a) = f(a^{-1})f(a).$$

Κι επειδή (λόγω το (v)) ισχύει $f(1_R) = 1_{f(R)} \neq 0_{R'}$, έχουμε $f(a) \neq 0_{R'}$ και $f(a^{-1}) = [f(a)]^{-1} \in f(R)^\times$. Η δεύτερη ισότητα αποδεικνύεται εύκολα μέσω μαθηματικής επαγωγής.

(ix) Έστω ότι ο f είναι μονομορφισμός και ο R ακεραία περιοχή. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Εάν υποθέσουμε ότι $f(a), f(b) \in f(R)$, για κάποια $a, b \in R$, τέτοια ώστε να ισχύει

$$f(a)f(b) = 0_{f(R)} \Longleftrightarrow f(ab) = 0_{f(R)} = f\left(0_R\right),$$

τότε $ab = 0_R$, οπότε $a = 0_R$ ή $b = 0_R$. Συνεπώς, $f(a) = 0_{f(R)}$ ή $f(b) = 0_{f(R)}$. Άρα *και* ο $f(R)$ είναι ακεραία περιοχή.

Εν συνεχεία, ας υποθέσουμε ότι ο f είναι μονομορφισμός και ο R στρεβλό σώμα. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Αρκεί λοιπόν να δείξουμε ότι $f(R)^\times = f(R) \smallsetminus \{0_{R'}\}$. Ο εγκλεισμός "$\subseteq$" είναι πρόδηλος. Ας θεωρήσουμε τυχόν $b \in f(R) \smallsetminus \{0_{R'}\}$. Τότε υπάρχει ένα $a \in R \smallsetminus \{0_R\}$, τέτοιο ώστε $b = f(a)$. Όμως -εξ υποθέσεως- $R \smallsetminus \{0_R\} = R^\times$, οπότε $a \in R^\times$, πράγμα που σημαίνει ότι υπάρχει (πολλαπλασιαστικό) αντίστροφο a^{-1} τού a, για το οποίο ισχύει $f(a^{-1}) = [f(a)]^{-1} \in f(R)^{\times}$ (βάσει τού (viii)). Άρα $b \in f(R)^{\times}$, και, ως εκ τούτου, ο $f(R)$ είναι στρεβλό σώμα. (Στην περίπτωση κατά την οποία ο f είναι μονομορφισμός και ο R σώμα, αρκεί να χρησιμοποιήσουμε ό,τι προείπαμε σε συνδυασμό με το (vii).) □

3.1.5 Πρόταση. *Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ομομορφισμοί (και αντιστοίχως, μονομορφισμοί/επιμορφισμοί/ισομορφισμοί) δακτυλίων, και η σύνθεσή τους $g \circ f : R \longrightarrow R''$ θα είναι ομομορφισμός (και αντιστοίχως, μονομορφισμός/επιμορφισμός/ισομορφισμός) δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Εάν οι f και g είναι ομομορφισμοί δακτυλίων, τότε για όλα τα $a, b \in R$ ισχύουν οι ισότητες

$$\begin{aligned}(g \circ f)(a+b) &= g(f(a+b)) = g(f(a) + f(b)) \\ &= g(f(a)) + g(f(b)) = (g \circ f)(a) + (g \circ f)(b)\end{aligned}$$

και

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) = g(f(a)f(b)) \\ &= g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b),\end{aligned}$$

οπότε και η σύνθεσή τους $g \circ f$ είναι ένας ομομορφισμός δακτυλίων. Η απόδειξη αποπερατούται λαμβάνοντας υπ' όψιν το γεγονός ότι η σύνθεση δυο ενρίψεων (και αντιστοίχως, επιρρίψεων/αμφιρρίψεων) είναι μια ένριψη (και αντιστοίχως, μια επίρριψη/αμφίρριψη). □

3.1.6 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι, τότε γράφουμε[2] $R \cong R'$ και λέμε ότι **ο R είναι ισόμορφος με τον R'** (ή ότι οι R και R' **είναι ισόμορφοι**) όταν υπάρχει κάποιος ισομορφισμός δακτυλίων $f : R \longrightarrow R'$. (Κατ' αναλογίαν, το σύμβολο $R \ncong R'$ δηλοί ότι ο δακτύλιος R *δεν είναι ισόμορφος* με τον R'.)

3.1.7 Παραδείγματα. (i) Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ (βλ. άσκηση **1-37**) είναι ισόμορφη με τον ακόλουθο δακτύλιο 2×2-πινάκων:

$$R := \left\{ \left(\begin{array}{cc} a & b \\ 2b & a \end{array} \right) \middle| \, a, b \in \mathbb{Z} \right\} \underset{\neq}{\subseteq} \mathrm{Mat}_{2\times 2}(\mathbb{Z}),$$

καθόσον υφίσταται ισομορφισμός δακτυλίων:

$$\mathbb{Z}[\sqrt{2}] \ni a + b\sqrt{2} \longmapsto \left(\begin{array}{cc} a & b \\ 2b & a \end{array} \right) \in R.$$

[2] Από τούδε και στο εξής μέσω τού συμβόλου "$\cong$" θα εκφράζουμε την ύπαρξη ισομορφισμών *δακτυλίων*. Ωστόσο, επειδή (στη Θεωρία Ομάδων) χρησιμοποιήσαμε το *ίδιο* σύμβολο *και* για τους ισομορφισμούς *ομάδων*, οφείλουμε να είμαστε ιδιάτερα προσεκτικοί (πρβλ. 3.1.2 παράδειγμα (ii)). Σε περίπτωσεις στις οποίες ενδέχεται να προκληθεί σύγχυση, θα μπορούσε κανείς να χρησιμοποιήσει τα (κάπως δυσμετακίνητα) σύμβολα $\underset{\text{δακτ.}}{\cong}$ και $\underset{\text{ομάδ.}}{\cong}$, αντιστοίχως.

(ii) Έχουμε $\mathbb{Z}[\sqrt{2}] \ncong \mathbb{Z}[\sqrt{3}]$, διότι εάν υπήρχε ισομορφισμός δακτυλίων

$$f : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}],$$

θα έπρεπε να ισχύει

$$f(\sqrt{2})^2 = f((\sqrt{2})^2) = f(2) = f(1+1) = 2f(1) = 2 \Rightarrow f(\sqrt{2}) \in \{\pm\sqrt{2}\},$$

κάτι που θα αντέφασκε προς το ότι $\pm\sqrt{2} \notin \mathbb{Z}[\sqrt{3}]$.

(iii) Τα σώματα $\mathbb{C}$ και $\mathbb{R}$ δεν είναι ισόμορφα, διότι εάν υπήρχε ένας ισομορφισμός $f : \mathbb{C} \longrightarrow \mathbb{R}$, τότε θα έπρεπε να ισχύει

$$-1 = -f(1) = f(-1) = f(i^2) = f(i)^2$$

(όπου i η φανταστική μονάδα), κάτι που θα αντέφασκε προς το ότι $f(i) \in \mathbb{R}$.

3.1.8 Πρόταση. *Για οιουσδήποτε δακτυλίους R, R', R'' ισχύουν τα εξής:*

(i) $R \cong R$,

(ii) $R \cong R' \Longrightarrow R' \cong R$,

(iii) $[R \cong R' \ \textit{και} \ R' \cong R''] \Longrightarrow R \cong R''$.

ΑΠΟΔΕΙΞΗ. (i) Η ταυτοτική απεικόνιση $\mathrm{id}_R : R \to R$ είναι προφανώς ένας ισομορφισμός δακτυλίων.

(ii) Εάν ο $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε, ως αμφιρριπτική απεικόνιση, θα διαθέτει μια (μονοσημάντως ορισμένη, αμφιρριπτική) αντίστροφο f^{-1}. Αρκεί λοιπόν να αποδειχθεί ότι η f^{-1} αποτελεί ομομορφισμό δακτυλίων. Εάν $x, y \in R'$, τότε υπάρχουν $a, b \in R$ με $x = f(a)$ και $y = f(b)$. Επομένως,

$$\begin{cases} f^{-1}(x+y) = f^{-1}(f(a)+f(b)) = f^{-1}(f(a+b)) = a+b = f^{-1}(x) + f^{-1}(y), \\ \\ f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)\, f^{-1}(y), \end{cases}$$

(αφού οι f, f^{-1} αμφιρριπτικές) και η f^{-1} είναι όντως ομομορφισμός δακτυλίων.

(iii) Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ισομορφισμοί δακτυλίων, τότε, σύμφωνα με την πρόταση 3.1.5, *και* η σύνθεσή τους $g \circ f$ είναι ένας ισομορφισμός δακτυλίων. □

3.1.9 Σημείωση. Σύμφωνα με την πρόταση 3.1.8, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από δακτυλίους (ή επί τής NBG-«κλάσεως» *όλων* των δακτυλίων). Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο δακτύλιοι λογίζονται ως (δακτυλιοθεωρητικώς) *ταυτιζόμενοι* όταν είναι μεταξύ τους ισόμορφοι, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο δακτυλιοθεωρητικός προσδιορισμός μιας οικογενείας δακτυλίων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού* [3].

3.1.10 Πόρισμα. *Εάν οι R και R' είναι δυο δακτύλιοι και $R \cong R'$, τότε ισχύουν τα εξής:*

(i) *Ο R είναι ακεραία περιοχή $\Leftrightarrow$ ο R' είναι ακεραία περιοχή.*

(ii) *Ο R είναι στεβλό σώμα $\Leftrightarrow$ ο R' είναι στεβλό σώμα.*

(iii) *Ο R είναι σώμα $\Leftrightarrow$ ο R' είναι σώμα.*

ΑΠΟΔΕΙΞΗ. Εάν η $f : R \longrightarrow R'$ είναι ένας ισομορφισμός δακτυλίων, τότε αρκεί να εφαρμοσθεί το (ix) τής προτάσεως 3.1.4 για αμφότερες τις f και f^{-1}. (Πρβλ. με το (ii) τής προτάσεως 3.1.8.) □

3.1.11 Πρόταση. *Εάν ο $f : K \longrightarrow R$ είναι ένας ομομορφισμός δακτυλίων, όπου ο K είναι ένας διαιρετικός δακτύλιος (= στρεβλό σώμα), τότε ο f είναι ή ο μηδενικός ομομορφισμός ή ένας μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Εάν ο R είναι τετριμμένος δακτύλιος, τότε ο f είναι κατ' ανάγκην ο μηδενικός ομομορφισμός. Εάν ο R είναι μη τετριμμένος δακτύλιος και ο f δεν είναι ο μηδενικός ομομορφισμός (ήτοι δεν ισχύει $f(a) = 0_R$, *για κάθε* $a \in K$), και εάν -επιπροσθέτως- υποθέσουμε ότι $f(x) = f(y)$ για κάποια $x, y \in K$, τότε

$$f(x-y) = f(x) - f(y) = 0_R. \tag{3.2}$$

Εάν $x-y \neq 0_K$, τότε το $x-y$ θα διαθέτει πολλαπλασιαστικό αντίστροφο $(x-y)^{-1}$. Αυτό, κατά το (viii) τής προτάσεως 3.1.4, σημαίνει ότι

$$f((x-y)^{-1}) \in f(K)^{\times}, \;\; f((x-y)^{-1}) = (f(x-y))^{-1}. \tag{3.3}$$

Από τις (3.2) και (3.3) συνάγουμε ότι $0_R = f(x-y)(f(x-y))^{-1} = 1_R$, πράγμα άτοπο. Επομένως, $x = y$, και ο f είναι κατ' ανάγκην μονομορφισμός. □

3.1.12 Πόρισμα. *Κάθε επιμορφισμός στρεβλών σωμάτων $f : K \longrightarrow L$ είναι ισομορφισμός.*

ΑΠΟΔΕΙΞΗ. Επειδή ο πληθικός αριθμός τού L είναι ≥ 2 και ο f επιμορφισμός, ο f αδυνατεί να είναι ο τετριμμένος ομομορφισμός. Κατά συνέπειαν, ο f οφείλει να είναι *και* ενριπτικός επί τη βάσει τής προτάσεως 3.1.11. □

[3] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (δακτυλίων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

3.1.13 Ορισμός. Εάν ο $f : R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων, τότε ο υποδακτύλιος $\mathrm{Ker}(f) := f^{-1}(\{0_{R'}\})$ τού R ονομάζεται **πυρήνας** τού f.

3.1.14 Πρόταση. *Ο πυρήνας* $\mathrm{Ker}(f)$ *ενός ομομορφισμού δακτυλίων* $f : R \to R'$ *αποτελεί ένα ιδεώδες τού* R.

ΑΠΟΔΕΙΞΗ. Έστω ότι $r \in R$ και ότι $a, b \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{array}{r} f(a-b) = f(a) - f(b) = 0_{R'} - 0_{R'} = 0_{R'}, \\ f(ar) = f(a)f(r) = 0_{R'}f(r) = 0_{R'}, \\ f(ra) = f(r)f(a) = f(r)0_{R'} = 0_{R'} \end{array}\right\} \Longrightarrow a-b,\ ar,\ ra \in \mathrm{Ker}(f).$$

Άρα ο $\mathrm{Ker}(f)$ είναι εξ ορισμού ένα ιδεώδες τού R. □

3.1.15 Πρόταση. *Έστω* $f : R \longrightarrow R'$ *ένας ομομορφισμός δακτυλίων. Τότε ο*

$$f \text{ είναι μονομορφισμός} \iff \mathrm{Ker}\,(f) = \{0_R\}\ .$$

ΑΠΟΔΕΙΞΗ. Εάν ο f είναι μονομορφισμός δακτυλίων και a είναι ένα τυχόν στοιχείο τού πυρήνα $\mathrm{Ker}(f)$, τότε

$$f(a) = 0_{R'} = f(0_R) \underset{f \text{ ένριψη}}{\Longrightarrow} a = 0_R.$$

Άρα $\mathrm{Ker}(f) = \{0_R\}$. Και αντιστρόφως· εάν ισχύει $\mathrm{Ker}(f) = \{0_R\}$ και υποθέσουμε ότι $f(x) = f(y)$, για κάποια $x, y \in R$, τότε

$$f(x-y) = f(x) - f(y) = 0_{R'} \Longrightarrow x - y \in \mathrm{Ker}(f) = \{0_R\} \Longrightarrow x - y = 0_R,$$

δηλαδή ο ομομορφισμός f είναι ενριπτικός. □

3.1.16 Ορισμός. Λέμε ότι ο δακτύλιος R μπορεί να **εμφυτευθεί** (ή ότι είναι **εμφυτεύσιμος**) σε έναν δακτύλιο R' όταν υπάρχει ένας μονομορφισμός δακτυλίων $f : R \longrightarrow R'$.

3.1.17 Πρόταση. *Ένας δακτύλιος* R *είναι εμφυτεύσιμος σε έναν δακτύλιο* R' *εάν και μόνον εάν ο* R *είναι ισόμορφος με έναν υποδακτύλιο τού* R'.

ΑΠΟΔΕΙΞΗ. Εάν ένας δακτύλιος R είναι εμφυτεύσιμος σε έναν δακτύλιο R', τότε υφίσταται κάποιος μονομορφισμός $f : R \longrightarrow R'$. Επομένως, ο μέσω αυτού επαγόμενος επιμορφισμός $\check{f} : R \longrightarrow \mathrm{Im}(f)$ (βλ. 3.1.2 (viii)) είναι ισομορφισμός. Και αντιστρόφως· εάν ο R είναι ισόμορφος με έναν υποδακτύλιο S τού R', τότε υφίσταται κάποιος ισομορφισμός $f : R \longrightarrow S$. Θεωρώντας (κατόπιν επεκτάσεως) ως πεδίο τιμών τής απεικονίσεως f το R' λαμβάνουμε τον μονομορφισμό δακτυλίων $R \ni r \longmapsto f(r) \in R'$. □

3.1.18 Πρόταση. *Κάθε δακτύλιος R μπορεί να εμφυτευθεί (όχι μονοσημάντως) σε έναν δακτύλιο R' με μοναδιαίο στοιχείο. Μάλιστα, ο R' μπορεί να επιλεγεί κατά τέτοιον τρόπο, ώστε* $\mathrm{χαρ}(R') = 0$ *ή* $\mathrm{χαρ}(R') = \mathrm{χαρ}(R)$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε το καρτεσιανό γινόμενο $R' := \mathbb{Z} \times R$, όπου $\mathbb{Z}$ ο δακτύλιος των ακεραίων αριθμών. Επί τού R' ορίζονται πράξεις προσθέσεως και πολλαπλασιασμού ως ακολούθως:

(i) $(m, a) + (n, b) := (m + n, a + b)$,

(ii) $(m, a) \cdot (n, b) := (mn, mb + na + ab)$,

για οιαδήποτε $(m, a), (n, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής 0 με μοναδιαίο του στοιχείο το $(1, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto (0, a)\,,$$

είναι ένας μονομορφισμός. Εάν $\mathrm{χαρ}(R) = k > 0$, τότε μπορούμε να θεωρήσουμε ως R' το καρτεσιανό γινόμενο $R' := \mathbb{Z}_k \times R$ εφοδιασμένο με τις πράξεις:

(i) $([m]_k\,, a) + ([n]_k\,, b) := ([m + n]_k\,, a + b)$,

(ii) $([m]_k\,, a) \cdot ([n]_k\,, b) := ([mn]_k\,, mb + na + ab)$,

για κάθε $([m]_k\,, a)$, $([n]_k\,, b) \in R'$. Η τριάδα $(R', +, \cdot)$ αποτελεί έναν δακτύλιο χαρακτηριστικής k με μοναδιαίο του στοιχείο το $([1]_k\,, 0_R)$, και η απεικόνιση

$$f : R \longrightarrow R', \quad a \longmapsto ([0]_k\,, a)\,,$$

είναι και πάλι ένας μονομορφισμός. □

3.1.19 Σημείωση. Πολλές φορές συμβαίνει «ειδικοί» δακτύλιοι να είναι εμφυτευμένοι σε δακτυλίους «ολιγότερο ειδικούς». Επί παραδείγματι, σώματα ενδέχεται να είναι εμφυτευμένα εντός στρεβλών σωμάτων, και ακέραιες περιοχές εντός δακτυλίων με μηδενοδιαιρέτες (βλ. 3.1.20 (i) και (ii)). Ωστόσο, όπως θα δούμε στην ενότητα 3.5 (βλ. πρόταση 3.5.7), *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί κατά τρόπο φυσικό σε ένα σώμα.

3.1.20 Παραδείγματα. (i) Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι εμφυτευμένο στο στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$ των (πραγματικών) τετρανίων (οπότε το $\mathbb{H}_{\mathbb{R}}$ μπορεί, υπό μία άποψη, να θεωρείται ως «φυσική επέκταση» τού $\mathbb{C}$) μέσω τού ακόλουθου μονομορφισμού:

$$\boxed{\mathbb{C} \hookrightarrow \mathbb{H}_{\mathbb{R}}, \ \ a + bi \longmapsto a\mathbf{I} + b\mathbf{J} = \begin{pmatrix} a + bi & 0 \\ 0 & a - bi \end{pmatrix},}$$

όπου οι $\mathbf{I}$ και $\mathbf{J}$ είναι οι πίνακες οι εισαχθέντες στο 1.2.19 (ii).

(ii) Εάν στην πρόταση 3.1.18 θέσουμε $R = \mathbb{Z}$ και $R' = \mathbb{Z}\times\mathbb{Z}$ (με τη δομή δακτυλίου την ορισθείσα κατά την αποδεικτική διαδικασία!), τότε ο R είναι ακεραία περιοχή, ενώ ο R' *δεν είναι*, διότι π.χ. για κάθε $n \in \mathbb{Z}\smallsetminus\{0\}$ ισχύει η ισότητα:

$$(-2,2)\,(,0,2n) = (0, 0-4n+4n) = (0,0).$$

► **Πηλικοδακτύλιοι και φυσικοί επιμορφισμοί**. Έστω R ένας δακτύλιος και έστω I ένα ιδεώδες αυτού. Θεωρούμε τον *πηλικοδακτύλιο* R/I (βλ. 2.6.1 και 2.6.2). Η απεικόνιση

$$\boxed{\pi_I^R : R \longrightarrow R/I,\;\; \pi_I^R(r) := r + I,\; \forall r \in R,} \tag{3.4}$$

είναι προφανώς επιρριπτική.

3.1.21 Λήμμα. *Η* (3.4) *αποτελεί έναν επιμορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τις (2.5) και (2.6). □

3.1.22 Ορισμός. Η (3.4) καλείται **φυσικός επιμορφισμός** (ή **επιμορφισμός κλάσεων υπολοίπων**) τού R επί τού πηλικοδακτυλίου R/I.

Η επόμενη πρόταση δηλοί -κατ' ουσίαν- ότι οι έννοιες «πυρήνας ομομορφισμού δακτυλίων» και «ιδεώδες» μπορούν να χρησιμοποιούνται η μία αντί τής άλλης χωρίς περαιτέρω περιορισμούς.

3.1.23 Πρόταση. *Έστω R τυχών δακτύλιος. Τότε ένα υποσύνολο $\varnothing \neq I \subseteq R$ αποτελεί ένα ιδεώδες τού R εάν και μόνον εάν το I είναι ο πυρήνας ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ (για κάποιον κατάλληλο δακτύλιο S).*

ΑΠΟΔΕΙΞΗ. Εάν $\varnothing \neq I \subseteq R$ είναι ένα ένα ιδεώδες τού R, τότε ο φυσικός επιμορφισμός (3.4) έχει ως πυρήνα του τον $\mathrm{Ker}(\pi_I^R) = \{r \in R \mid r + I = I\} = I$. Το αντίστροφο είναι άμεση συνέπεια τής προτάσεως 3.1.14. □

3.1.24 Πόρισμα. *Ο φυσικός επιμορφισμός* (3.4) *είναι ισομορφισμός εάν και μόνον εάν $I = \{0_R\}$.*

ΑΠΟΔΕΙΞΗ. Σύμφωνα με την πρόταση 3.1.15 ο $\pi_I^R : R \longrightarrow R/I$ είναι μονομορφισμός εάν και μόνον εάν ο πυρήνας του (που ισούται με το I) είναι το τετριμμένο ιδεώδες. □

3.1.25 Πόρισμα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο R είναι ένα σώμα.*

(ii) *Τα μόνα ιδεώδη τού R είναι το $\{0_R\}$ και ο ίδιος ο R.*

(iii) *Το $\{0_R\}$ είναι μεγιστικό ιδεώδες τού R.*

(iv) *Κάθε μη μηδενικός ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ είναι μονομορφισμός.*

ΑΠΟΔΕΙΞΗ. Η αμφίπλευρη συνεπαγωγή (i)⇔(ii) έπεται από το πόρισμα 2.1.11, η (i)⇔(iii) από το πόρισμα 2.6.5 (αφού $R \cong R/\{0_R\}$, βλ. 3.1.10 (iii) και 3.1.24) και η συνεπαγωγή (i)⇒(iv) από την πρόταση 3.1.11. Για την απόδειξη τής συνεπαγωγής (iv)⇒(ii) αρκεί να θεωρήσουμε *τυχόν* ιδεώδες $I \subsetneqq R$ και τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$, ο οποίος είναι μη μηδενικός με $\mathrm{Ker}(\pi_I^R) = I$. Εάν υποθέσουμε ότι ο π_I^R είναι μονομορφισμός, έχουμε $I = \{0_R\}$, οπότε ο R δεν διαθέτει άλλα γνήσια ιδεώδη πέραν τού τετριμμένου. Η απόδειξη λήγει ακολουθώντας τις συνεπαγωγές (iv)⇒(ii)⇒(i). □

3.2 ΘΕΩΡΗΜΑ ΑΝΤΙΣΤΟΙΧΙΣΕΩΣ ΙΔΕΩΔΩΝ

3.2.1 Λήμμα. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Εάν υποτεθεί ότι το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και το J ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού S, τότε ισχύουν τα ακόλουθα:*

(i) *Η εικόνα $f(I)$ τού I μέσω τού f είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού δακτυλίου $f(R)$.*

(ii) *Η αντίστροφη εικόνα $f^{-1}(J)$ τού J μέσω τού f είναι ένα (αριστερό/ δεξιό/αμφίπλευρο) ιδεώδες τού R.*

ΑΠΟΔΕΙΞΗ. (i) Θεωρούμε τυχόντα στοιχεία $s \in f(R)$ και $x, y \in f(I)$. Επειδή το I είναι (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R, υπάρχουν $r \in R$, $a, b \in I$, τέτοια ώστε $s = f(r)$, $x = f(a)$ και $y = f(b)$, και ισχύουν τα ακόλουθα:

$$\left.\begin{array}{r} x - y = f(a) - f(b) = f(a-b) \in f(I), \\ sx = f(r)f(a) = f(ra) \in f(I) \mid xs = f(ar) \in f(I) \mid sx, xs \in f(I) \end{array}\right\}$$

απ' όπου έπεται ότι η εικόνα $f(I)$ τού I μέσω τού f είναι ένα (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού δακτυλίου $f(R)$.

(ii) Θεωρούμε τυχόντα στοιχεία $r \in R$ και $a, b \in f^{-1}(J)$. Τότε, επειδή το J είναι (αριστερό και, αντιστοίχως, δεξιό/αμφίπλευρο) ιδεώδες τού S,

$$\left.\begin{array}{r} f(a-b) = f(a) - f(b) \in J, \\ f(ra) = f(r)f(a) \in J \mid f(ar) = f(a)f(r) \in J \mid f(ra), f(ar) \in J \end{array}\right\}$$

απ' όπου έπεται ότι $a - b,\ ra \mid ar \mid ra, ar \in f^{-1}(J)$. Άρα το $f^{-1}(J)$ είναι εξ ορισμού ένα ομοειδές ιδεώδες τού R. □

3.2.2 Σημείωση. Εάν υποτεθεί ότι το I είναι ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R και ότι ο f δεν είναι επιμορφισμός, η εικόνα $f(I)$ τού I μέσω τού f είναι ένα ομοειδές ιδεώδες τού δακτυλίου $f(R)$ αλλά όχι κατ' ανάγκην και τού S. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, η εικόνα τού ιδεώδους $I := 2\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών μέσω αυτής είναι το υποσύνολο $2\mathbb{Z}$ τού $\mathbb{Q}$ που *δεν είναι ιδεώδες* τού σώματος των ρητών αριθμών (καθότι τα μόνα ιδεώδη τού $\mathbb{Q}$ είναι τα $\{0\}$ και $\mathbb{Q}$, βλ. πόρισμα 2.1.11).

3.2.3 Πρόταση. *Έστω I ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες ενός δακτυλίου R και έστω J ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες ενός δακτυλίου S. Για κάθε ομομορφισμό δακτυλίων $f : R \longrightarrow S$ ισχύουν τα εξής:*
(i) $f\left(I \cap f^{-1}(J)\right) = f(I) \cap J$.
(ii) $f\left(f^{-1}(J)\right) = \mathrm{Im}(f) \cap J$.
(iii) $f^{-1}(J + f(I)) = f^{-1}(J) + I$.
(iv) $f^{-1}(f(I)) = \mathrm{Ker}(f) + I$.

ΑΠΟΔΕΙΞΗ. (i) Για κάθε $r \in f^{-1}(J)$ έχουμε $f(r) \in J$, οπότε $f\left(f^{-1}(J)\right) \subseteq J$. Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής τής απεικονίσεως f, έχουμε

$$\left.\begin{array}{r} f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \\ f\left(I \cap f^{-1}(J)\right) \subseteq f\left(f^{-1}(J)\right) \end{array}\right\} \Longrightarrow f\left(I \cap f^{-1}(J)\right) \subseteq f(I) \cap J.$$

Έστω τώρα τυχόν $s \in f(I) \cap J$. Προφανώς, $s \in J$ και $s = f(r)$ για κάποιο στοιχείο $r \in I$. Επειδή $f(r) \in J$, έχουμε $s \in f\left(I \cap f^{-1}(J)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f(I) \cap J \subseteq f\left(I \cap f^{-1}(J)\right).$$

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $I = R$.
(iii) Για κάθε $a \in I$ έχουμε $f(a) \in f(I)$. Επομένως, $I \subseteq f^{-1}(f(I))$. Από το (ii) και από το γεγονός ότι οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν θεωρήσεως αντιστρόφων εικόνων προκύπτει ότι

$$f^{-1}(J) + I \subseteq f^{-1}\left(f(f^{-1}(J) + I)\right) = f^{-1}\left(f(f^{-1}(J)) + f(I)\right) \subseteq f^{-1}(J + f(I)).$$

Έστω τώρα τυχόν $r \in f^{-1}(J + f(I))$. Επειδή $f(r) \in J + f(I)$, υπάρχουν $s \in J$ και $b \in I$, τέτοια ώστε $f(r) = s + f(b)$. Κατά συνέπειαν,

$$f(r + (-b)) = s \in J \Rightarrow r + (-b) \in f^{-1}(s) \subseteq f^{-1}(J) \Rightarrow r \in f^{-1}(J) + I,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός

$$f^{-1}(J + f(I)) \subseteq f^{-1}(J) + I.$$

(iv) Αρκεί να εφαρμοσθεί το (iii) στην ειδική περίπτωση όπου $J = \{0_S\}$. □

3.2.4 Θεώρημα τής αντιστοιχίσεως. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων και έστω $W := \mathrm{Ker}(f)$. Τότε η*

$$\left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } R\\ \text{που περιέχουν τον } W\end{array}\right\} \xrightarrow{\alpha} \left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } S\end{array}\right\}$$

η οριζόμενη από τον τύπο

$$\boxed{I \longmapsto \alpha(I) := f(I)}$$

είναι μια αμφίρριψη που διατηρεί τους εγκλεισμούς, δηλαδή για οιαδήποτε ιδεώδη I_1, I_2 τού R ισχύει η συνεπαγωγή

$$W \subseteq I_1 \subsetneqq I_2 \Longrightarrow \alpha(I_1) \subsetneqq \alpha(I_2).$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε την

$$\left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } S\end{array}\right\} \xrightarrow{\beta} \left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } R\\ \text{που περιέχουν τον } W\end{array}\right\}$$

την οριζόμενη από τον τύπο

$$J \longmapsto \beta(J) := f^{-1}(J).$$

Το ότι οι α, β είναι καλώς ορισμένες απεικονίσεις έπεται από το λήμμα 3.2.1. Για κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες J τού S λαμβάνουμε

$$\alpha(\beta(J)) = \alpha(f^{-1}(J)) = f(f^{-1}(J)) = \mathrm{Im}(f) \cap J = S \cap J = J$$

(βλ. 3.2.3 (ii)). Κατά συνέπειαν,

$$\alpha(\beta(J)) = J. \tag{3.5}$$

Από την άλλη μεριά, για κάθε ιδεώδες (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες I τού R που περιέχει τον πυρήνα W τού f λαμβάνουμε

$$\beta(\alpha(I)) = \beta(f(I)) = f^{-1}(f(I)) = W + I = I$$

(βλ. 3.2.3 (iv)). Κατά συνέπειαν,

$$\beta(\alpha(I)) = I. \tag{3.6}$$

Από τις (3.5) και (3.6) συμπεραίνουμε ότι η απεικόνιση α είναι αμφιρριπτική έχουσα την β ως αντίστροφό της. Τέλος, ας υποθέσουμε ότι τα I_1, I_2 είναι δυο (αριστερά/δεξιά/αμφίπλευρα) ιδεώδη τού R τα οποία περιέχουν τον W και για τα οποία ισχύει ο εγκλεισμός $I_1 \subsetneqq I_2$. Προφανώς, $f(I_1) \subseteq f(I_2)$. Κι επειδή

$$f(I_1) = f\left(I_2\right) \Rightarrow I_1 = f^{-1}(f(I_1)) = f^{-1}(f(I_2)) = I_2,$$

έχουμε $\alpha(I_1) = f(I_1) \subsetneqq f(I_2) = \alpha(I_1)$. □

3.2.5 Πόρισμα. *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε κάθε ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής J/I, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το I.*

Απόδειξη. Θεωρούμε τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$ (βλ. (3.4)). Βάσει τού θεωρήματος 3.2.4 τής αντιστοιχίσεως ιδεωδών κάθε ιδεώδες τού R/I είναι τής μορφής $\pi_I^R\left(J\right)$, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το $I = \mathrm{Ker}(\pi_I^R)$ (βλ. πρόταση 3.1.23). Το I είναι και αυτό ένα ιδεώδες τού J (όταν το J θεωρηθεί αφ' εαυτού ως δακτύλιος αναφοράς), ενώ η εικόνα $\pi_I^R\left(J\right)$ ισούται με

$$\pi_I^R\left(J\right) = \left\{\pi_I^R\left(a\right) \;\middle|\; a \in J\right\} = \{a + I \mid a \in J\} = J/I,$$

απ' όπου έπεται το ζητούμενο. □

3.2.6 Παράδειγμα. Για $R = \mathbb{Z}$ και $I = m\mathbb{Z}$, $m \in \mathbb{N}$, το σύνολο των ιδεωδών τού πηλικοδακτυλίου $\mathbb{Z}/m\mathbb{Z}$ είναι το

$$\{\, d\mathbb{Z}/m\mathbb{Z} |\; d \in \mathbb{N} \text{ και } d \mid m \,\}\,.$$

3.3 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Αυτά είναι τρία χαρακτηριστικά θεωρήματα (βλ. 3.3.3, 3.3.15 και 3.3.20) τα οποία περιγράφουν τον τρόπο διασυνδέσεως των ομομορφισμών δακτυλίων, των ιδεωδών δακτυλίων και των πηλικοδακτυλίων. Τα εξ αυτών εξαγόμενα πορίσματα είναι πολιποίκιλα και λίαν χρήσιμα.

3.3.1 Λήμμα. *Εάν τα A, B είναι μη κενά σύνολα και η $\pi : A \longrightarrow B$ μια απεικόνιση, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η π είναι επιρριπτική απεικόνιση.*

(ii) *Υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$.*

(iii) *Η π είναι «εκ δεξιών διαγράψιμη», δηλαδή για οιοδήποτε μη κενό σύνολο C και οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ ισχύει η συνεπαγωγή*

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η π είναι επιρριπτική απεικόνιση, τότε για κάθε στοιχείο $y \in B = \mathrm{Im}(\pi) = \pi(A)$ επιλέγουμε ένα $x_y \in A$, ούτως ώστε να ισχύει $\pi(x_y) = y$, και ορίζουμε την απεικόνιση $\gamma : B \longrightarrow A,\ y \longmapsto \gamma(y) := x_y$. Τότε

$$(\pi \circ \gamma)(y) = \pi(\gamma(y)) = \pi(x_y) = y = \mathrm{id}_B(y) \Longrightarrow \pi \circ \gamma = \mathrm{id}_B.$$

(ii)⇒(iii) Υποθέτουμε ότι υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\pi \circ \gamma = \mathrm{id}_B$. Για οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ για τις οποίες ισχύει η ισότητα $h_1 \circ \pi = h_2 \circ \pi$ λαμβάνουμε

$$\begin{aligned} h_1 \circ \pi &= h_2 \circ \pi \Rightarrow (h_1 \circ \pi) \circ \gamma = (h_2 \circ \pi) \circ \gamma \\ &\Rightarrow h_1 \circ (\pi \circ \gamma) = h_2 \circ (\pi \circ \gamma) \\ &\Rightarrow h_1 = h_1 \circ \mathrm{id}_B = h_2 \circ \mathrm{id}_B = h_2. \end{aligned}$$

(iii)⇒(i) Υποθέτουμε ότι η π είναι «εκ δεξιών διαγράψιμη». Εάν το B είναι μονοσύνολο, τότε η π είναι προδήλως επιρριπτική. Εάν το B περιέχει τουλάχιστον δύο στοιχεία y_1, y_2 με $y_1 \neq y_2$, τότε ορίζουμε τις απεικονίσεις

$$h_1(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_1, & \text{όταν } y \notin \mathrm{Im}(\pi), \end{cases} \quad h_2(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(\pi), \\ y_2, & \text{όταν } y \notin \mathrm{Im}(\pi). \end{cases}$$

Προφανώς, $h_1(\pi(x)) = \pi(x) = h_2(\pi(x))$ για κάθε $x \in X$, οπότε

$$h_1 \circ \pi = h_2 \circ \pi \Longrightarrow h_1 = h_2.$$

Εάν υπήρχε κάποιο $y \in B \smallsetminus \mathrm{Im}(\pi)$, τότε θα ίσχυε

$$h_1(y) = h_2(y) \Longrightarrow y_1 = y_2,$$

ήτοι κάτι που θα αντέκειτο προς την υπόθεσή μας. Επομένως, $B = \mathrm{Im}(\pi)$. $\square$

3.3.2 Θεώρημα. («Καθολική ιδιότητα πηλικοδακτυλίου») *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε για κάθε ομομορφισμό δακτυλίων $g : R \longrightarrow S$ για τον οποίον ισχύει $I \subseteq \mathrm{Ker}(g)$, η*

$$\boxed{h : R/I \longrightarrow S,\ \ a + I \longmapsto h(a + I) := g(a),\ \forall a \in R,}$$

είναι καλώς ορισμένη απεικόνιση και αποτελεί έναν ομομορφισμό δακτυλίων. Αυτός είναι ο μόνος ομομορφισμός από τον πηλικοδακτύλιο R/I στον δακτύλιο S που καθιστά το διάγραμμα

$$\begin{tikzcd} R \arrow[r, "g"] \arrow[d, "\pi_I^R"'] \arrow[dr, phantom, "\circlearrowleft"] & S \\ R/I \arrow[ur, "h"'] & \end{tikzcd}$$

μεταθετικό (ήτοι $h \circ \pi_I^R = g$). Επιπροσθέτως, ισχύουν τα ακόλουθα:
(i) *Ο h είναι μονομορφισμός $\Longleftrightarrow I = \mathrm{Ker}(g)$.*
(ii) *Ο h είναι επιμορφισμός $\Longleftrightarrow$ ο g είναι επιμορφισμός.*

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς η h είναι καλώς ορισμένη απεικόνιση, διότι εάν έχουμε $a + I = b + I$, για κάποια $a, b \in R$, τότε

$$a - b \in I \subseteq \mathrm{Ker}\,(g) \Longrightarrow g(a-b) = g(a) - g(b) = 0_{R'} \Longrightarrow g(a) = g(b).$$

Επίσης, $h \circ \pi_I^R = g$, καθότι ισχύει

$$h\left(\pi_I^R\,(a)\right) = h\,(a+I) = g\,(a)\,,\ \ \forall a \in R.$$

Το ότι η h είναι και ομομορφισμός δακτυλίων συνάγεται από τις ακόλουθες ισότητες:

$$\begin{cases} h\,((a+I)+(b+I)) = h\,((a+b)+I) = g(a+b) \\ = g(a)+g(b) = h\,(a+I) + h\,(b+I)\,, \\ h\,((a+I)\,(b+I)) = h\,(ab+I) = g(ab) \\ = g(a)g(b) = h\,(a+I)\,h\,(b+I)\,,\ \forall (a,b) \in R \times R. \end{cases}$$

Ο ομομορφισμός h είναι ο μόνος ομομορφισμός από τον R/I στον S που καθιστά το ως άνω διάγραμμα μεταθετικό. Πράγματι· εάν $h' : R/I \longrightarrow S$ είναι *τυχών* ομομορφισμός δακτυλίων με $h' \circ \pi_I^R = g$, τότε (σύμφωνα με τη συνεπαγωγή (i)⇒(iii) τού λήμματος 3.3.1)

$$h \circ \pi_I^R = h' \circ \pi_I^R \Longrightarrow h = h'.$$

(i) Υποθέτουμε ότι ο h είναι μονομορφισμός. Έστω τυχόν $a \in \mathrm{Ker}(g)$. Τότε

$$h\,(a+I) = g(a) = 0_S = h\left(0_{R/I}\right) = h\,(I) \underset{[h \text{ ένριψη}]}{\Longrightarrow} a + I = I \Longrightarrow a \in I.$$

Άρα $\mathrm{Ker}(g) \subseteq I$. Κι επειδή (εξ υποθέσεως) $I \subseteq \mathrm{Ker}(g)$, έχουμε $\mathrm{Ker}(g) = I$.
Και αντιστρόφως· εάν υποθέσουμε ότι $\mathrm{Ker}(g) = I$, αρκεί να δείξουμε (επί τη βάσει τής προτάσεως 3.1.15) ότι $\mathrm{Ker}(h) = \{0_{R/I}\}$. Έστω λοιπόν τυχόν $a + I \in \mathrm{Ker}(h)$. Τότε

$$g(a) = h\,(a+I) = 0_S \Longrightarrow a \in \mathrm{Ker}\,(g) = I \Longrightarrow a + I = I = 0_{R/I},$$

απ' όπου έπεται ότι πράγματι $\mathrm{Ker}(h) = \{0_{R/I}\}$.
(ii) Εάν ο h είναι επιμορφισμός, τότε και ο $g = h \circ \pi_I^R$ είναι επιμορφισμός (ως σύνθεση δύο επιμορφισμών). Και αντιστρόφως· εάν ο $g = h \circ \pi_I^R$ είναι επιμορφισμός και $s \in S$, τότε υπάρχει κάποιο $r \in R$, τέτοιο ώστε να ισχύει $g(r) = s$. Άρα το $\pi_I^R(r)$ απεικονίζεται μέσω τής h στο s και ο h είναι επιμορφισμός. □

3.3.3 Πρώτο Θεώρημα Ισομορφισμών. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε*

$$\boxed{R/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f) = f\,(R)\,.}$$

Συγκεκριμένα, η απεικόνιση

$$\begin{aligned} h : R/\mathrm{Ker}(f) &\longrightarrow \mathrm{Im}\,(f) = f\,(R) \\ a + \mathrm{Ker}(f) &\longmapsto h(a + \mathrm{Ker}(f)) := f\,(a)\,, \end{aligned}$$

είναι (ο μόνος) ισομορφισμός δακτυλίων που καθιστά το διάγραμμα

$$\begin{tikzcd}
R \arrow[r, "\check{f}"] \arrow[d, "\pi^{R}_{\mathrm{Ker}(f)}"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathrm{Im}(f) \\
R/\mathrm{Ker}(f) \arrow[ur, "h"'] &
\end{tikzcd}$$

μεταθετικό, όπου $\check{f}$ ο επιμορφισμός ο επαγόμενος μέσω τού f (βλ. 3.1.2 (viii)).

Αποδειξη. Εφαρμόζουμε το θεώρημα 3.3.2 για το ιδεώδες $I := \mathrm{Ker}(f)$ τού R και για τον επιμορφισμό $g := \check{f}$. (Εν προκειμένω, η προϋποτεθείσα συνθήκη αυτού τού θεωρήματος ικανοποιείται, διότι $\mathrm{Ker}(f) = \mathrm{Ker}(\check{f})$.) Μάλιστα, ο κατασκευαζόμενος ομομορφισμός h είναι μονομορφισμός. Από την άλλη μεριά, η απεικόνιση h είναι, συν τοις άλλοις, και επιρριπτική, καθόσον για κάθε $s \in \mathrm{Im}(f)$ υπάρχει κάποιο $r \in R$ με $s = \check{f}(r) = f(r)$, οπότε $h(r + \mathrm{Ker}(f)) = s$. $\square$

3.3.4 Παραδείγματα. (i) Έστω $m \in \mathbb{N}$ και έστω f ο επιμορφισμός δακτυλίων

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, \;\; n \longmapsto [n]_m\,, \;\; \forall n \in \mathbb{Z}.$$

Τότε

$$\begin{aligned} \mathrm{Ker}\,(f) &= \{r \in \mathbb{Z} \mid f(r) = [0]_m\} = \{r \in \mathbb{Z} \mid [r]_m = [0]_m\} \\ &= \{r \in \mathbb{Z} \mid r = km, \; k \in \mathbb{Z}\} = \{km \mid k \in \mathbb{Z}\} = m\mathbb{Z}, \end{aligned}$$

και, σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.3, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Εξάλλου, επειδή $m\mathbb{Z} = -m\mathbb{Z}$ για κάθε $m \in \mathbb{Z} \smallsetminus \{0\}$, έχουμε γενικότερα

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|}, \; \forall m \in \mathbb{Z} \smallsetminus \{0\}.} \tag{3.7}$$

(ii) Έστω R ο υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ ο οριζόμενος ως εξής:

$$R := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix} \right) \,\middle|\, a, b \in \mathbb{R} \right\},$$

και έστω f η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{R}, \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix} \right) \longmapsto a.$$

Τότε -όπως κανείς μπορεί εύκολα να ελέγξει- η f είναι ομομορφισμός δακτυλίων, οπότε, δυνάμει τού 1ου θεωρήματος ισομορφισμών 3.3.3,

$$\boxed{R/I \cong \mathbb{R},}$$

όπου

$$I = \mathrm{Ker}(f) = \left\{ \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix} \right) \,\middle|\, b \in \mathbb{R} \right\}.$$

(iii) Έστω R ο υποδακτύλιος τού σώματος $\mathbb{Q}$ των ρητών αριθμών ο οριζόμενος ως εξής:

$$R := \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, a \in \mathbb{Z},\ b \in \mathbb{Z}\diagdown\{0\} \ \text{και} \ \text{μκδ}\,(a,b) = 1,\ b \equiv 1 (\mathrm{mod}\, 2) \right\}.$$

Η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{Z}_2,\ \tfrac{a}{b} \longmapsto f(\tfrac{a}{b}) := \begin{cases} [0]_2, & \text{όταν } a \equiv 0 (\mathrm{mod}\, 2), \\ [1]_2, & \text{όταν } a \equiv 1 (\mathrm{mod}\, 2), \end{cases}$$

είναι ομομορφισμός δακτυλίων (γιατί;) και (βάσει τού 1ου θεωρήματος ισομορφισμών 3.3.3)

$$\boxed{R/\left\{ \tfrac{a}{b} \in R \,\middle|\, a \equiv 0 (\mathrm{mod}\, 2) \right\} \cong \mathbb{Z}_2.}$$

(iv) Ο επιμορφισμός δακτυλίων

$$\mathbb{Z}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto a_0 \in \mathbb{Z}$$

έχει ως πυρήνα του το κύριο ιδεώδες

$$\left\{ \sum_{i=0}^{n} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \,\middle|\, a_0 = 0 \right\} = \langle \mathsf{X} \rangle,$$

οπότε

$$\boxed{\mathbb{Z}[\mathsf{X}]/\langle \mathsf{X} \rangle \cong \mathbb{Z}.}$$

Επί τη βάσει των (i) και (iii) τού πορίσματος 3.1.10, τού θεωρήματος 2.6.4 και τού πορίσματος 2.6.5 το $\langle \mathsf{X} \rangle$ είναι πρώτο, μη μεγιστικό ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$.

3.3.5 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και το I ένα ιδεώδες τού R, τέτοιο ώστε $\mathrm{Ker}(f) \subseteq I$. Τότε*

$$\boxed{R/I \cong S/f(I).}$$

ΑΠΟΔΕΙΞΗ. Κατά το (i) τού λήμματος 3.2.1 η εικόνα $f(I)$ τού ιδεώδους I μέσω τού f είναι ένα ιδεώδες τού S, οπότε μπορεί να ορισθεί ο πηλικοδακτύλιος $S/f(I)$. Έστω $\pi^S_{f(I)} : S \longrightarrow S/f(I)$ ο φυσικός επιμορφισμός. Η απεικόνιση

$$g = \pi^S_{f(I)} \circ f : R \longrightarrow S/f(I)$$

είναι ένας επιμορφισμός δακτυλίων (ως σύνθεση δύο επιμορφισμών, βλ. 3.1.5) με πυρήνα του το ιδεώδες

$$\begin{aligned}
\mathrm{Ker}\,(g) &= \left\{a \in R \mid g(a) = 0_{S/f(I)}\right\} \\
&= \left\{a \in R \mid \pi^S_{f(I)}(f(a)) = f(I)\right\} \\
&= \{a \in R \mid f(a) + f(I) = f(I)\} \\
&= \{a \in R \mid f(a) \in f(I)\} \\
&= f^{-1}(f(I)),
\end{aligned}$$

το οποίο ισούται με το I (διότι $\mathrm{Ker}(f) \subseteq I$, βλ. θεώρημα 3.2.4). Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.3 για την g. □

3.3.6 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και το J ένα ιδεώδες τού S. Τότε*

$$\boxed{R/f^{-1}(J) \cong S/J.}$$

ΑΠΟΔΕΙΞΗ. Έστω $\pi^S_J : S \longrightarrow S/J$ ο φυσικός επιμορφισμός. Η απεικόνιση $g = \pi^S_J \circ f : R \longrightarrow S/J$ είναι ένας επιμορφισμός δακτυλίων (ως σύνθεση δύο επιμορφισμών, βλ. 3.1.5), με πυρήνα του το ιδεώδες

$$\begin{aligned}
\mathrm{Ker}\,(g) &= \left\{a \in R \mid g(a) = 0_{S/J}\right\} \\
&= \left\{a \in R \mid \pi^S_J(f(a)) = J\right\} \\
&= \{a \in R \mid f(a) + J = J\} \\
&= \{a \in R \mid f(a) \in J\} \\
&= f^{-1}(J).
\end{aligned}$$

Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.3 για την g. □

3.3.7 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής:*

(i) *Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{p})$ είναι ένα πρώτο ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{q})$ είναι ένα πρώτο ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

ΑΠΟΔΕΙΞΗ. (i) Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου R που περιέχει τον πυρήνα τού f, τότε ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή και $R/\mathfrak{p} \cong S/f(\mathfrak{p})$ (λόγω τού θεωρήματος 2.6.4 και τού πορίσματος 3.3.5). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{p})$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 3.1.10). Αυτό σημαίνει ότι το $f(\mathfrak{p})$ οφείλει να είναι πρώτο ιδεώδες τού S (εκ νέου λόγω τού θεωρήματος 2.6.4).

(ii) Εάν το $\mathfrak{q}$ είναι ένα πρώτο ιδεώδες τού δακτυλίου S, τότε ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή και $S/\mathfrak{q} \cong R/f^{-1}(\mathfrak{q})$ (λόγω τού θεωρήματος 2.6.4, τού πορίσματος 3.3.6 και τού (ii) τής προτάσεως 3.1.8). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι ακεραία περιοχή (βλ. το (i) τού πορίσματος 3.1.10). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{q})$ οφείλει να είναι πρώτο ιδεώδες τού δακτυλίου R (εκ νέου λόγω τού θεωρήματος 2.6.4). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{q}$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{q})$. □

3.3.8 Πόρισμα. (Θεώρημα αντιστοιχίσεως για πρώτα ιδεώδη.)
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα πρώτα φάσματα

$$\mathrm{Spec}(R) := \{\,\mathfrak{p} |\, \mathfrak{p} \text{ πρώτο ιδεώδες τού } R\}\,,\ \mathrm{Spec}(S) := \{\,\mathfrak{q} |\, \mathfrak{q} \text{ πρώτο ιδεώδες τού } S\}$$

των R και S (βλ. άσκηση **2-36**). *Εάν* $\mathrm{Spec}(S) \neq \varnothing$, *τότε η*

$$\boxed{\begin{array}{ccc} \mathbf{V}(W) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq W\} & \longrightarrow & \mathrm{Spec}(S) \\ \mathfrak{p} & \longmapsto & f(\mathfrak{p}) \end{array}} \tag{3.8}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \Longrightarrow f(\mathfrak{p}_1) \subsetneqq f(\mathfrak{p}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.7, για κάθε $\mathfrak{p} \in \mathbf{V}(W)$ έχουμε $f(\mathfrak{p}) \in \mathrm{Spec}(S)$ και για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ έχουμε $f^{-1}(\mathfrak{q}) \in \mathbf{V}(W)$. Επειδή $\mathfrak{p} = f^{-1}(f(\mathfrak{p}))$ για κάθε $\mathfrak{p} \in \mathbf{V}(W)$ και $\mathfrak{q} = f(f^{-1}(\mathfrak{q}))$ για κάθε $\mathfrak{q} \in \mathrm{Spec}(S)$ (βλ. απόδειξη τού θεωρήματος 3.2.4), η (3.8) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός $\alpha|_{\mathbf{V}(W)}$ τής α τής ορισθείσας στο θεώρημα 3.2.4 επί τού $\mathbf{V}(W)$). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.4. □

3.3.9 Σημείωση. Εάν ο $f : R \longrightarrow S$ ένας ομομορφισμός (όχι κατ' ανάγκην επιμορφισμός!) μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, τότε

$$f^{-1}(\mathfrak{q}) \in \operatorname{Spec}(R), \;\; \forall \mathfrak{q} \in \operatorname{Spec}(S),$$

οπότε, υπό την προϋπόθεση ότι $\operatorname{Spec}(S) \neq \varnothing$, ο f επάγει μια «κανονιστική» απεικόνιση (σε επίπεδο πρώτων φασμάτων):

$$\operatorname{Spec}(S) \ni \mathfrak{q} \longmapsto f^{-1}(\mathfrak{q}) \in \operatorname{Spec}(R).$$

Πράγματι· η αντίστροφη εικόνα $f^{-1}(\mathfrak{q})$ οιουδήποτε $\mathfrak{q} \in \operatorname{Spec}(S)$ είναι ένα ιδεώδες τού R (βλ. 3.2.1 (ii)), ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή (βλ. θεώρημα 2.6.4) και η εφαρμογή τού 1ου θεωρήματος ισομορφισμών 3.3.3 για τη σύνθεση $\pi_{\mathfrak{q}}^{S} \circ f$ των ομομορφισμών

$$R \xrightarrow{f} S \xrightarrow{\pi_{\mathfrak{q}}^{S}} S/\mathfrak{q}$$

δίδει τον ισομορφισμό

$$R/\operatorname{Ker}(\pi_{\mathfrak{q}}^{S} \circ f) \cong \operatorname{Im}(\pi_{\mathfrak{q}}^{S} \circ f) \subseteq S/\mathfrak{q}.$$

Επειδή (σύμφωνα με το (iii) τής προτάσεως 3.1.4) η εικόνα $\operatorname{Im}(\pi_{\mathfrak{q}}^{S} \circ f)$ είναι ένας υποδακτύλιος τής ακεραίας περιοχής $S/\mathfrak{q}$ και

$$1_{S/\mathfrak{q}} = 1_S + \mathfrak{q} = \pi_{\mathfrak{q}}^{S}(1_S) = \pi_{\mathfrak{q}}^{S}(f(1_R)) = (\pi_{\mathfrak{q}}^{S} \circ f)(1_R) = 1_{\operatorname{Im}(\pi_{\mathfrak{q}}^{S} \circ f)}$$

(βλ. 3.1.4 (v)), η πρόταση 1.2.20 μας πληροφορεί ότι η $\operatorname{Im}(\pi_{\mathfrak{q}}^{S} \circ f)$ είναι ακεραία περιοχή, οπότε και ο πηλικοδακτύλιος $R/\operatorname{Ker}(\pi_{\mathfrak{q}}^{S} \circ f)$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 3.1.10). Επιπροσθέτως, επειδή

$$\begin{aligned} \operatorname{Ker}(\pi_{\mathfrak{q}}^{S} \circ f) &= \left\{ r \in R \mid \pi_{\mathfrak{q}}^{S}\left(f\left(r\right)\right) = 0_{S/\mathfrak{q}} \right\} \\ &= \left\{ r \in R \mid f\left(r\right) + \mathfrak{q} = \mathfrak{q} \right\} \\ &= \left\{ r \in R \mid f\left(r\right) \in \mathfrak{q} \right\} = f^{-1}(\mathfrak{q}), \end{aligned}$$

ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι μια ακεραία περιοχή, οπότε έχουμε κατ' ανάγκην $f^{-1}(\mathfrak{q}) \in \operatorname{Spec}(R)$ (βλ. θεώρημα 2.6.4).

3.3.10 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε πρώτο ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{p}/I$, όπου $\mathfrak{p}$ κάποιο (μονοσημάντως ορισμένο) πρώτο ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα πορίσματα 3.3.8 και 3.2.5. □

3.3.11 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Τότε ισχύουν τα εξής:*

(i) *Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε το $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού S.*

(ii) *Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε το $f^{-1}(\mathfrak{m}')$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f.*

ΑΠΟΔΕΙΞΗ. (i) Εάν το $\mathfrak{m}$ είναι ένα μεγιστικό ιδεώδες τού R που περιέχει τον πυρήνα τού f, τότε ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι σώμα και $R/\mathfrak{m} \cong S/f(\mathfrak{m})$ (λόγω των πορισμάτων 2.6.5 και 3.3.5). Άρα και ο πηλικοδακτύλιος $S/f(\mathfrak{m})$ είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.10). Αυτό σημαίνει ότι το $f(\mathfrak{m})$ οφείλει να είναι μεγιστικό ιδεώδες τού S (εκ νέου λόγω τού πορίσματος 2.6.5).

(ii) Εάν το $\mathfrak{m}'$ είναι ένα μεγιστικό ιδεώδες τού S, τότε ο πηλικοδακτύλιος $S/\mathfrak{m}'$ είναι σώμα και $S/\mathfrak{m}' \cong R/f^{-1}(\mathfrak{m}')$ (λόγω των πορισμάτων 2.6.5 και 3.3.5, και τού (ii) τής προτάσεως 3.1.8). Άρα και ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{m}')$ είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.10). Αυτό σημαίνει ότι το $f^{-1}(\mathfrak{m}')$ οφείλει να είναι μεγιστικό ιδεώδες τού R (εκ νέου λόγω τού πορίσματος 2.6.5). Επιπροσθέτως, $\{0_S\} \subseteq \mathfrak{m}'$, οπότε $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{m}')$. □

Εν συνεχεία, παραθέτουμε ένα πόρισμα ανάλογο τού 3.3.8 *για μεγιστικά ιδεώδη*.

3.3.12 Πόρισμα. (Θεώρημα αντιστοιχίσεως για μεγιστικά ιδεώδη.)
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα ***μεγιστικά φάσματα***

$$\text{Max-Spec}(R) := \left\{ \mathfrak{m} \,\middle|\, \begin{array}{c} \mathfrak{m} \text{ μεγιστικό} \\ \text{ιδεώδες τού } R \end{array} \right\}, \ \text{Max-Spec}(S) := \left\{ \mathfrak{n} \,\middle|\, \begin{array}{c} \mathfrak{n} \text{ μεγιστικό} \\ \text{ιδεώδες τού } S \end{array} \right\}$$

των R και S. Εάν ο S είναι μη τετριμμένος, τότε η

$$\boxed{\begin{array}{ccc} \{\mathfrak{m} \in \text{Max-Spec}(R) \,|\, \mathfrak{m} \supseteq W\} & \longrightarrow & \text{Max-Spec}(S) \\ \mathfrak{m} & \longmapsto & f(\mathfrak{m}) \end{array}} \tag{3.9}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$W \subseteq \mathfrak{m}_1 \subsetneqq \mathfrak{m}_2 \Longrightarrow f(\mathfrak{m}_1) \subsetneqq f(\mathfrak{m}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.11, η εικόνα $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού δακτυλίου S για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και το $f^{-1}(\mathfrak{m}')$ είναι μεγιστικό ιδεώδες τού R περιέχον τον W για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού

S. Επειδή $\mathfrak{m} = f^{-1}(f(\mathfrak{m}))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}$ τού R με $\mathfrak{m} \supseteq W$ και $\mathfrak{m}' = f(f^{-1}(\mathfrak{m}'))$ για κάθε μεγιστικό ιδεώδες $\mathfrak{m}'$ τού S (βλ. απόδειξη τού θεωρήματος 3.2.4), η (3.9) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός τής α τής ορισθείσας στο θεώρημα 3.2.4 επί τού συνόλου των μεγιστικών ιδεωδών τού R που περιέχουν τον W). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.4. $\square$

3.3.13 Σημείωση. Έστω $f : R \longrightarrow S$ ένας ομομορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$. Εάν ο f δεν είναι επιμορφισμός, τότε, σε αντίθεση με ό,τι συμβαίνει στην περίπτωση θεωρήσεως αντιστρόφων εικόνων πρώτων ιδεωδών (βλ. 3.3.9), η αντίστροφη εικόνα ενός μεγιστικού ιδεώδους τού S μέσω τού f δεν είναι κατ' ανάγκην μεγιστικό ιδεώδες τού R. Επί παραδείγματι, θεωρώντας τή συνήθη ένθεση $\mathrm{in}_{\mathbb{Z},\mathbb{Q}} : \mathbb{Z} \hookrightarrow \mathbb{Q}$, παρατηρούμε ότι η $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}$ είναι μονομορφισμός, δεν είναι επιμορφισμός, $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}(1) = 1$, το τετριμμένο ιδεώδες $\{0\}$ τού $\mathbb{Q}$ είναι μεγιστικό (βλ. πόρισμα 2.1.11), αλλά η αντίστροφη εικόνα $\mathrm{in}_{\mathbb{Z},\mathbb{Q}}^{-1}(\{0\}) = \{0\}$ τού $\{0\}$ είναι το τετριμμένο ιδεώδες τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών που *δεν είναι μεγιστικό ιδεώδες* (βλ. 2.5.23 (i)).

3.3.14 Πόρισμα. *Έστω I ένα γνήσιο ιδεώδες ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Τότε κάθε μεγιστικό ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής $\mathfrak{m}/I$, όπου $\mathfrak{m}$ κάποιο (μονοσημάντως ορισμένο) μεγιστικό ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα πορίσματα 3.3.12 και 3.2.5. $\square$

3.3.15 Δεύτερο Θεώρημα Ισομορφισμών. *Έστω ότι ο R είναι ένας δακτύλιος, ο S ένας υποδακτύλιος τού R και το I ένα ιδεώδες τού R. Τότε*

(i) *το $S \cap I$ είναι ένα ιδεώδες τού S,*

(ii) *το $S + I := \{\, s + a \mid s \in S,\ a \in I\}$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$,*

(iii) *το I είναι ένα ιδεώδες τού $S + I$ και*

(iv) *υφίσταται ισομορφισμός δακτυλίων*

$$\boxed{S/(S \cap I) \cong (S + I)/I.}$$

ΑΠΟΔΕΙΞΗ. (i) Επειδή το I είναι ένα ιδεώδες τού R, έχουμε

$$\{0_S\} = \{0_R\} \subseteq S \cap I \subseteq S.$$

Επίσης, το $S \cap I$ αποτελεί προσθετική υποομάδα τής (αβελιανής) ομάδας $(S, +)$. Έστω τώρα τυχόν $a \in S \cap I$. Προφανώς, $a \in S$ και $a \in I$. Επειδή $a \in S$ και ο S είναι υποδακτύλιος τού R, ισχύει

$$sa \in S,\ \ as \in S,\ \forall s \in S,$$

λόγω τής κλειστότητας τής πράξεως τού πολλαπλασιασμού εντός τού S. Από την άλλη μεριά, επειδή το I είναι ιδεώδες τού R,

$$sa \in I, \;\; as \in I.$$

Επομένως, $sa, as \in S \cap I$ για κάθε $s \in S$ και κάθε $a \in S \cap I$. Εξ αυτών έπεται ότι το $S \cap I$ είναι ένα ιδεώδες τού S.

(ii) Εάν $s \in S$, τότε προφανώς $s + 0_R \in S + I$, αφού $0_R \in I$. Άρα $S \subseteq S + I$. Εν συνεχεία, ας υποθέσουμε ότι $x_1, x_2 \in S + I$. Τα x_1, x_2 γράφονται ως $x_1 = s_1 + a_1$ και $x_2 = s_2 + a_2$, για κάποια $s_1, s_2 \in S$ και $a_1, a_2 \in I$. Επομένως,

$$\left.\begin{array}{r} x_1x_2 = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2, \\ s_1s_2 \in S, \\ s_1a_2 + a_1s_2 + a_1a_2 \in I \end{array}\right\} \Longrightarrow x_1x_2 \in S + I,$$

και

$$\left.\begin{array}{r} x_1 - x_2 = (s_1 - s_2) + (a_1 - a_2)\,, \\ s_1 - s_2 \in S, \\ a_1 - a_2 \in I \end{array}\right\} \Longrightarrow x_1 - x_2 \in S + I.$$

Άρα τελικώς το $S + I$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$.

(iii) Έστω ότι $a, b \in I$ και $x = s + c \in S + I$, όπου $s \in S$ και $c \in I$. Τότε ο ισχυρισμός είναι αληθής λόγω τής συνεπαγωγής:

$$\left.\begin{array}{r} a - b \in I \quad (\text{διότι το } I \text{ είναι ιδεώδες τού } R) \\ sa \in I \quad (\text{διότι } s \in R \text{ και το } I \text{ είναι ιδεώδες τού } R) \\ ca \in I \quad (\text{διότι το } I \text{ είναι υποδακτύλιος τού } R) \end{array}\right\} \Longrightarrow a - b, \;\; xa \in I.$$

(iv) Έστω f η απεικόνιση

$$f : S \longrightarrow (S + I)/I, \;\; s \longmapsto s + I, \;\; \forall s \in S.$$

Προφανώς, $f = \pi_I^{S+I} \circ j$, όπου $\pi_I^{S+I} : S + I \longrightarrow (S + I)/I$ ο επιμορφισμός κλάσεων υπολοίπων και $j : S \longrightarrow S + I$ η συνήθης ένθεση $s \longmapsto s\,(+0_R)$. Κατά το 1ο θεώρημα ισομορφισμών 3.3.3, $S/\mathrm{Ker}(f) \cong f(S)$. Θα αποδείξουμε εν πρώτοις ότι $\mathrm{Ker}(f) = S \cap I$. Έστω λοιπόν τυχόν $s \in \mathrm{Ker}(f)$. Τότε

$$\left.\begin{array}{r} f(s) = s + I = 0_R + I \Longrightarrow s \in I \\ s \in S \end{array}\right\} \Longrightarrow s \in S \cap I.$$

Και αντιστρόφως· εάν $s \in S \cap I$, τότε $f(s) = s + I = 0_R + I = I \Longrightarrow s \in \mathrm{Ker}(f)$. Άρα πράγματι $\mathrm{Ker}(f) = S \cap I$. Ως εκ τούτου, αρκεί να αποδειχθεί η ισότητα:

$f(S) = (S+I)/I$ (ήτοι ότι η f είναι επιρριπτική). Έστω τυχόν $b + I \in (S+I)/I$. Τότε $b = s + a$, για κάποια $s \in S$ και $a \in I$. Επομένως,

$$I \ni (s+a) - s = a \Longrightarrow f(s) = s + I = s + a + I = b + I,$$

πράγμα που επιβεβαιώνει την επιρριπτικότητα τής f. □

3.3.16 Πόρισμα. *Έστω ότι ο R είναι ένας δακτύλιος και τα I, J δύο ιδεώδη του. Τότε υφίστανται ισομορφισμοί* :

$$\boxed{I/\left(I \cap J\right) \cong \left(I+J\right)/J}$$

και

$$\boxed{\left(I+J\right)/\left(I \cap J\right) \cong \left(\left(I+J\right)/I\right) \times \left(\left(I+J\right)/J\right) \cong \left(J/\left(I \cap J\right)\right) \times \left(I/\left(I \cap J\right)\right).}$$

Απόδειξη. Ο πρώτος ισομορφισμός είναι άμεσος δυνάμει τού 2ου θεωρήματος ισομορφισμών 3.3.15. Για την απόδειξη των άλλων δύο ισομορφισμών ορίζουμε την

$$f : I + J \longrightarrow \left(\left(I+J\right)/I\right) \times \left(\left(I+J\right)/J\right), \;\; a \longmapsto \left(a+I, a+J\right), \; \forall a \in I+J.$$

Είναι εύκολος ο έλεγχος τού ότι η f αποτελεί ομομομορφισμό δακτυλίων. Ο πυρήνας της ισούται προφανώς με

$$\begin{aligned} \mathrm{Ker}(f) &= \left\{a \in I+J \mid f(a) = 0_{((I+J)/I)\times((I+J)/J)}\right\} \\ &= \left\{a \in I+J \mid (a+I, a+J) = (I,J)\right\} \\ &= \left\{a \in I+J \mid a \in I, \; a \in J\right\} = I \cap J. \end{aligned}$$

Εν συνεχεία, θα δείξουμε ότι η f είναι επιρριπτική. Έστω τυχόν

$$\left(a+I, b+J\right) \in \left(\left(I+J\right)/I\right) \times \left(\left(I+J\right)/J\right).$$

Τότε τα a, b γράφονται ως αθροίσματα

$$a = u + v, \;\; b = w + z,$$

για κατάλληλα $u, w \in I$ και $v, z \in J$. Κατά συνέπειαν,

$$\begin{aligned} f(v) &= (v+I, v+J) = (v+I, 0_{I+J} + J), \\ f(w) &= (w+I, w+J) = (0_{I+J} + I, w+J), \end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$f(v+w) = f(v) + f(w) = (v+I, w+J) = (u+v+I, w+z+J) = (a+I, b+J),$$

δηλαδή ότι η f είναι επιμορφισμός με $\mathrm{Ker}(f) = I \cap J$. Αρκεί η εφαρμογή τού 1ου θεωρήματος ισομορφισμών. Τέλος, ο τρίτος -κατά σειράν- ισομορφισμός έπεται κατόπιν απευθείας εφαρμογής τού 2ου θεωρήματος ισομορφισμών 3.3.15 σε αμφότερους τους παράγοντες τού μετέχοντος καρτεσιανού γινομένου δακτυλίων. □

3.3.17 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle m \rangle$, $J = \langle n \rangle$, όπου $m, n \in \mathbb{Z} \smallsetminus \{0\}$, τότε, λαμβάνοντας υπ' όψιν τα όσα αποδείξαμε στα 2.4.13 (i), (ii), οι ισομορφισμοί οι θεσπισθέντες μέσω τού πορίσματος 3.3.16 γράφονται υπό τη μορφή:

$$\langle m \rangle \,/\, \langle \text{εκπ}(m,n) \rangle \cong \langle \text{μκδ}(m,n) \rangle \,/\, \langle n \rangle$$

και, αντιστοίχως,

$$\begin{aligned} \langle \text{μκδ}(m,n) \rangle \,/\, \langle \text{εκπ}(m,n) \rangle &\cong (\langle \text{μκδ}(m,n) \rangle \,/\, \langle m \rangle) \times (\langle \text{μκδ}(m,n) \rangle \,/\, \langle n \rangle) \\ &\cong (\langle n \rangle \,/\, \langle \text{εκπ}(m,n) \rangle) \times (\langle m \rangle \,/\, \langle \text{εκπ}(m,n) \rangle)\,. \end{aligned}$$

3.3.18 Ορισμός. Εάν τα I, J είναι δυο ιδεώδη ενός δακτυλίου R και ισχύει η ισότητα $R = I + J$, τότε λέμε ότι είναι τα I και J είναι **συμπρώτα**.

3.3.19 Πόρισμα. *Εάν τα I, J είναι συμπρώτα ιδεώδη ενός δακτυλίου R, τότε*

$$\boxed{R/\,(I \cap J) \cong (R/I) \times (R/J)\,.}$$

3.3.20 Τρίτο Θεώρημα Ισομορφισμών. *Εάν ο R είναι ένας δακτύλιος και τα I, J γνήσια ιδεώδη τού R με $I \subseteq J$, τότε έχουμε*

$$\boxed{R/J \cong (R/I)\,/\,(J/I).}$$

ΑΠΟΔΕΙΞΗ. Έστω f η απεικόνιση

$$f : R \longrightarrow (R/I)\,/\,(J/I)\,,\ \ a \longmapsto (a+I) + (J/I),\ \forall a \in R.$$

Επειδή $f = \pi^{R/I}_{J/I} \circ \pi^R_I$, όπου $\pi^R_I : R \longrightarrow (R/I)$ και $\pi^{R/I}_{J/I} : R/I \longrightarrow (R/I)\,/\,(J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.3,

$$R/\mathrm{Ker}\,(f) \cong (R/I)\,/\,(J/I)\,.$$

Όμως

$$\begin{aligned}
\mathrm{Ker}(f) &= \left\{ a \in R \mid f(a) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \left\{ a \in R \mid \pi^{R/I}_{J/I}(\pi^R_I(a)) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \left\{ a \in R \mid \pi^{R/I}_{J/I}(a+I) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \left\{ a \in R \mid a+I \in \mathrm{Ker}(\pi^{R/I}_{J/I}) \right\} \\
&= \{ a \in R \mid a+I \in (J/I) \} = J,
\end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

3.3.21 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle 12 \rangle = 12\mathbb{Z} \subsetneqq J = \langle 3 \rangle = 3\mathbb{Z}$, τότε, επειδή το ιδεώδες $3\mathbb{Z}/12\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}/12\mathbb{Z}$ περιέχει εκείνες τις κλάσεις υπολοίπων τού $\mathbb{Z}/12\mathbb{Z}$, οι εκπρόσωποι των οποίων ανήκουν στο $J = 3\mathbb{Z}$, ήτοι είναι πολλαπλάσια τού 3, έχουμε $J/I = \{I,\ 3+I,\ 6+I,\ 9+I\}$ και

$$(\mathbb{Z}/I)\ /\,(J/I) = \{ k + I + (J/I) \mid k \in \mathbb{Z},\ \ 0 \le k \le 11 \}\,.$$

Σημειωτέον ότι υπάρχουν πολλαπλές εμφανίσεις μεταξύ αυτών των δώδεκα στοιχείων, καθότι

$$\begin{aligned}
&(k_1 + I) - (k_2 + I) \in J/I \Longleftrightarrow (k_1 - k_2) + I \in J/I \\
&\Longleftrightarrow 3 \mid k_1 - k_2.
\end{aligned}$$

Ως εκ τούτου, ο δακτύλιος $(\mathbb{Z}/I)\ /\,(J/I)$ συνίσταται από ακριβώς τρεις σαφώς διακεκριμένες κλάσεις ισοτιμίας:

$$(\mathbb{Z}/I)\ /\,(J/I) = \{ k + I + (J/I) \mid k \in \mathbb{Z},\ \ 0 \le k \le 2 \}\,.$$

Κατά το 1ο και το 3ο θεώρημα ισομορφισμών (βλ. 3.3.3 και 3.3.20),

$$\mathbb{Z}_3 = \{[0]_3\,, [1]_3\,, [2]_3\} \cong \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cong} (\mathbb{Z}/I)\ /\,(J/I) = \{(J/I, 1 + (J/I), 2 + (J/I)\}.$$

3.4 ΕΦΑΡΜΟΓΗ: ΛΥΣΕΙΣ ΣΥΣΤΗΜΑΤΩΝ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Στην ενότητα 3.3 παρετέθησαν ορισμένα πρώτα παραδείγματα εφαρμογής των θεωρημάτων ισομορφισμών δακτυλίων (βλ. 3.3.4, 3.3.17 και 3.3.21). Εδώ θα παρουσιασθεί μια επιπρόσθετη, αρκούντως σημαντική εφαρμογή *αριθμοθεωρητικής φύσεως* σχετιζόμενη με τον προσδιορισμό τού συνόλου των λύσεων συστημάτων πεπερασμένου πλήθους γραμμικών ισοτιμιών (με έναν άγνωστο). Το κύριο θεώρημα τής παρούσας ενότητας είναι το 3.4.10, το επονομαζόμενο *Κινέζικο θεώρημα* [4] ή *θεώρημα τού Νικομάχου τού Γερασηνού* [5], για το οποίο δίνουμε μια καθαρώς «δακτυλιοθεωρητική» απόδειξη (αν και στη γενίκευσή του 3.4.15 δεν παραλείπουμε και την παράθεση μιας πιο «στοιχειώδους» προσβάσεως).

► **Γραμμικές ισοτιμίες**. Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b δυο ακέραιοι αριθμοί. Κάθε ισοτιμία τής μορφής

$$\boxed{ax \equiv b (\operatorname{mod} m),} \tag{3.10}$$

με το x προσδιοριστέο εντός τού συνόλου των ακεραίων αριθμών, καλείται **γραμμική ισοτιμία** (με *άγνωστό της* τον x). Λέμε ότι ένας $x_0 \in \mathbb{Z}$ *πληροί* (ή *επαληθεύει*) την (3.10) όταν $ax_0 \equiv b (\operatorname{mod} m)$. Εν τοιαύτη περιπτώσει, *και οιοσδήποτε άλλος* εκπρόσωπος τής κλάσεως υπολοίπων $[x_0]_m$ τού x_0 επαληθεύει την (3.10). Πράγματι· εάν $y \in [x_0]_m$, τότε $[y]_m = [x_0]_m$, απ' όπου έπεται ότι $y \equiv x_0 (\operatorname{mod} m)$, οπότε

$$ay \equiv ax_0 \equiv b (\operatorname{mod} m).$$

Ως εκ τούτου, όταν ομιλούμε για μια **λύση** $x_0 \in \mathbb{Z}$ **τής** (3.10) **κατά μόδιο** m, εννοούμε ολόκληρη[6] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (3.10). Επίσης, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα και συναντούμε μια λύση $[x_0]_m$, προτιμούμε να παραθέτουμε τον *μοναδικό* εκπρόσωπο x_0' τής κλάσεως υπολοίπων $[x_0]_m$ ο οποίος ανήκει στο σύνολο $\{0, 1, \ldots, m-1\}$, ήτοι να καταφεύγουμε σε *αναγωγή* τού x_0 κατά μόδιο m κατόπιν διαιρέσεώς του διά τού m.

Σημειωτέον ότι υπάρχουν γραμμικές ισοτιμίες οι οποίες δεν δέχονται καμία ακεραία λύση, όπως π.χ. η $2x \equiv 3 (\operatorname{mod} 4)$, αφού για κάθε $k \in \mathbb{Z}$ ο ακέραιος $2k-3$ είναι περιττός και επομένως $4 \nmid 2k-3$. Η πρόταση που ακολουθεί μας γνωστοποιεί την ικανή και αναγκαία συνθήκη για την ύπαρξη ακεραίων λύσεων τής (3.10) και, επιπροσθέτως, περιγράφει τη μορφή όλων των δυνατών λύσεων.

3.4.1 Πρόταση. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (3.10) *διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν* μκδ$(a, m) \mid b$.

[4] Παρότι στη βιβλιογραφία είναι γνωστό ως *Chinese remainder theorem,* πιθανολογείται πως οι Κινέζοι μαθηματικοί τού 3ου μ.Χ. αιώνα, οι οποίοι έδωσαν μια πρακτική μέθοδο επιλύσεως ενός συστήματος τριών γραμμικών ισοτιμιών, είχαν λάβει γνώση τού έργου τού Νικομάχου τού Γερασηνού, αφού το εν λόγω σύστημα περιέχει τους ίδιους αριθμούς με εκείνους τού Νικομάχου! Η πρώτη ολοκληρωμένη απόδειξη τού θεωρήματος 3.4.10 οφείλεται στον L. Euler, ενώ μια νεότερη απόδειξη ανακαλύφθηκε (μάλλον ανεξαρτήτως) από τον C.-F. Gauss περί το έτος 1801.

[5] Ο φιλόσοφος και μαθηματικός *Νικόμαχος ο Γερασηνός* (από τα Γέρασα, μια αρχαιοελληνική πόλη στην Παλαιστίνη, 30 μίλια νοτιοανατολικά τής λίμνης Τιβεριάδος, ιδρυθείσα από τον Μ. Αλέξανδρο) θα πρέπει -εξ όσων γνωρίζουμε- να έζησε σε κάποιο διάστημα μεταξύ τού μέσου τού 1ου και τού μέσου τού 2ου μ.Χ. αιώνα. Πέραν τής γνωστής του «Αριθμητικής Εισαγωγής» είχε συγγράψει και πολλά άλλα έργα, εκ των οποίων ελάχιστα τμήματα διεσώθησαν. Σε ένα όμως εξ αυτών παρατίθεται η λύση τού συστήματος των ισοτιμιών $x \equiv 2 (\operatorname{mod} 3)$, $x \equiv 3 (\operatorname{mod} 5)$ και $x \equiv 2 (\operatorname{mod} 7)$. (Για να την προσδιορίσετε, εφαρμόστε τό 3.4.10!)

[6] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (3.10) λογίζονται ως *διαφορετικές* όταν $x_1 \not\equiv x_2 (\operatorname{mod} m)$.

Επιπροσθέτως, όταν $\text{μκδ}\,(a,m)|\,b$, *η ισοτιμία* (3.10) *διαθέτει ακριβώς* $\text{μκδ}(a,m)$ *σαφώς διακεκριμένες λύσεις* $x \in \mathbb{Z}$ *κατά μόδιο* m, *οι οποίες είναι τής μορφής*

$$\boxed{x = x_0 + k\,\frac{m}{\text{μκδ}\,(a,m)}, \quad k \in \{0,1,\ldots,\text{μκδ}\,(a,m)-1\},} \tag{3.11}$$

όπου x_0 *μια ειδική λύση τής* (3.10).

Απόδειξη. Εάν η (3.10) δέχεται μια λύση $x \in \mathbb{Z}$ κατά μόδιο m, τότε

$$ax \equiv b(\text{mod } m) \Longrightarrow m \mid ax - b \Longrightarrow (\exists k \in \mathbb{Z} : b = ax - km)\,.$$

Επομένως,

$$\left.\begin{array}{r} \text{μκδ}\,(a,m) \mid a \\ \text{μκδ}\,(a,m) \mid m \end{array}\right\} \Longrightarrow \text{μκδ}\,(a,m) \mid ax - km\;(=b).$$

Και αντιστρόφως· εάν $\text{μκδ}(a,m) \mid b$, τότε $b = \text{μκδ}(a,m)\,b'$ για κάποιον $b' \in \mathbb{Z}$. Επειδή

$$\text{μκδ}\left(\tfrac{a}{\text{μκδ}(a,m)}, \tfrac{m}{\text{μκδ}(a,m)}\right) = 1 \Longrightarrow \left(\exists \kappa, \lambda \in \mathbb{Z} : \kappa\tfrac{a}{\text{μκδ}(a,m)} + \lambda\tfrac{m}{\text{μκδ}(a,m)} = 1\right),$$

λαμβάνουμε

$$b = \kappa\tfrac{ab}{\text{μκδ}(a,m)} + \lambda\tfrac{mb}{\text{μκδ}(a,m)} = a\,(\kappa b') + m\,(\lambda b') \Longrightarrow a\,(\kappa b') \equiv b(\text{mod } m),$$

οπότε η κλάση ισοτιμίας τού $\kappa b'$ κατά μόδιο m είναι μια λύση τής (3.10).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (3.10). Προφανώς,

$$a\left(x_0 + k\frac{m}{\text{μκδ}\,(a,m)}\right) = ax_0 + \left(\frac{ak}{\text{μκδ}\,(a,m)}\right)m \equiv b(\text{mod } m),$$

οπότε οι ακέραιοι (3.11) αποτελούν πράγματι λύσεις τής (3.10). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε ακεραίους αριθμούς $k, k' \in \{0,1,\ldots,\text{μκδ}(a,m)-1\}$ με $k \neq k'$, έχουμε

$$\left|\left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right)\right| = |k - k'|\;\tfrac{m}{\text{μκδ}(a,m)} < m,$$

αφού $|k-k'| < \text{μκδ}(a,m)$. Συνεπώς,

$$\begin{gathered} m \nmid \left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right) \\ \Downarrow \\ \left(x_0 + \tfrac{mk}{\text{μκδ}(a,m)}\right) \not\equiv \left(x_0 + \tfrac{mk'}{\text{μκδ}(a,m)}\right) (\text{mod } m). \end{gathered}$$

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y \in \mathbb{Z}$ τής (3.10) είναι ισότιμη με κάποια εκ των (3.11) κατά μόδιο m. Επειδή

$$\left.\begin{array}{r} ax_0 \equiv b(\mathrm{mod}\ m) \\ ay \equiv b(\mathrm{mod}\ m) \end{array}\right\} \Longrightarrow ax_0 \equiv ay(\mathrm{mod}\ m) \Longrightarrow m \mid a\,(y - x_0)\,,$$

συμπεραίνουμε ότι

$$\left.\begin{array}{r} \frac{m}{\text{μκδ}(a,m)} \mid \frac{a}{\text{μκδ}(a,m)}\,(y - x_0) \\ \text{μκδ}\left(\frac{a}{\text{μκδ}(a,m)}, \frac{m}{\text{μκδ}(a,m)}\right) = 1 \end{array}\right\} \Longrightarrow \begin{array}{c} \frac{m}{\text{μκδ}(a,m)} \mid y - x_0 \\ \Downarrow \\ \left(\exists \nu \in \mathbb{Z} : y - x_0 = \frac{m\nu}{\text{μκδ}(a,m)}\right). \end{array}$$

Διαιρώντας τον ν διά τού μκδ(a, m) λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q, r) \in \mathbb{Z}^2$ με

$$\nu = \text{μκδ}\,(a, m)\,q + r, \quad 0 \leq r \leq \text{μκδ}\,(a, m) - 1.$$

Ως εκ τούτου,

$$y - x_0 = \frac{m(\text{μκδ}(a,m)q+r)}{\text{μκδ}(a,m)} = mq + \frac{rm}{\text{μκδ}(a,m)} \equiv \frac{rm}{\text{μκδ}(a,m)}(\mathrm{mod}\ m),$$

οπότε $y \equiv x_0 + r\frac{m}{\text{μκδ}(a,m)}(\mathrm{mod}\, m), \forall r \in \{0, 1, \ldots, \text{μκδ}(a, m) - 1\}$. □

3.4.2 Πόρισμα. *Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία* (3.10) *διαθέτει ακριβώς μία λύση x_0 κατά μόδιο m εάν και μόνον εάν* μκδ$\,(a, m) = 1$.

3.4.3 Σημείωση. Όταν μκδ$(a, m) = 1$, ένας τρόπος υπολογισμού τής λύσεως x_0 κατά μόδιο m διασφαλίζεται μέσω τής προσφυγής μας στον κλασικό *ευκλείδειο αλγόριθμο* (ήτοι στον προσδιορισμό ενός ζεύγους $(x_0^*, y_0^*) \in \mathbb{Z}^2$ για το οποίο ισχύει $ax_0^* - my_0^* = 1$, ορίζοντας ως x_0 το $x_0 := bx_0^*$). Ένας άλλος τρόπος υπολογισμού τής λύσεως x_0 είναι δυνατός κατόπιν εφαρμογής τού θεωρήματος τού Euler περί ισοτιμιών. Σύμφωνα με αυτό, (λόγω τής συνθήκης μκδ$(a, m) = 1$) έχουμε

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\ m),$$

όπου ϕ η συνάρτηση φι τού Euler. Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\phi(m)-1}b,} \tag{3.12}$$

να εφαρμόσουμε τον γνωστό τύπο ευρέσεως τού $\phi\,(m)$ για τον δοθέντα φυσικό αριθμό m και να διενεργήσουμε αναγωγή κατά μόδιο m.

3.4.4 Παράδειγμα. Επειδή μκδ$(5, 24) = 1$, η γραμμική ισοτιμία $5x \equiv 3(\mathrm{mod}\ 24)$ διαθέτει *ακριβώς μία* λύση x_0 κατά μόδιο m. Γράφοντας $24 = 2^3 \cdot 3$, διαπιστώνουμε άμεσα ότι $\phi(24) = (2^3 - 2^2)(3-1) = 8$. Κατά τον (3.12), μπορούμε να θέσουμε ως $x_0 := 5^7 \cdot 3 = 234\,375$. Επειδή $234\,375 = 9765 \cdot 24 + 15$, έχουμε $[x_0]_{24} = [15]_{24}$, οπότε $5 \cdot 15 \equiv 3(\mathrm{mod}\ 24)$.

Η εύρεση των λύσεων τής γενικής γραμμικής ισοτιμίας (3.10) ανάγεται -κατ' ουσίαν- στην ειδική περίπτωση που περιγράψαμε στα 3.4.2 και 3.4.3, ως ακολούθως:

3.4.5 Πόρισμα. *Δοθέντων ενός* $m \in \mathbb{N}$ *και δυο ακεραίων* a, b, $a \neq 0$, *με* μκδ$(a, m) | b$, *η γραμμική ισοτιμία* (3.10) *διαθέτει* μκδ(a, m) *λύσεις* $x \in \mathbb{Z}$ *κατά μόδιο* m, *οι οποίες είναι τής μορφής* (3.11), *όπου* x_0 *η μοναδική λύση κατά μόδιο* $\frac{m}{\text{μκδ}(a,m)}$ *τής*

$$\left(\frac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\frac{b}{\text{μκδ}(a,m)}\right) (\mathrm{mod}\ \left(\frac{m}{\text{μκδ}(a,m)}\right)). \tag{3.13}$$

Απόδειξη. Θέτοντας $\widetilde{a} := \frac{a}{\text{μκδ}(a,m)}$, $\widetilde{b} := \frac{b}{\text{μκδ}(a,m)}$ και $\widetilde{m} := \frac{m}{\text{μκδ}(a,m)}$, έχουμε μκδ$(\widetilde{a}, \widetilde{m}) = 1$, καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} ax \equiv b\ (\mathrm{mod}\ m) &\iff \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b}\ (\mathrm{mod}\ \text{μκδ}\,(a,m)\,\widetilde{m}) \\ &\iff \widetilde{a}x \equiv \widetilde{b}\ (\mathrm{mod}\ \widetilde{m}) \\ &\iff \left(\frac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\frac{b}{\text{μκδ}(a,m)}\right)\ (\mathrm{mod}\ \left(\frac{m}{\text{μκδ}(a,m)}\right)), \end{aligned}$$

διότι μκδ$(a, m) \neq 0$, οπότε η (3.13) ισοδυναμεί με την (3.10). □

3.4.6 Παράδειγμα. Η γραμμική ισοτιμία

$$6x \equiv 3(\mathrm{mod}\,21)$$

διαθέτει μκδ$(6, 21) = 3$ λύσεις κατά μόδιο 21 τής μορφής $x_0, x_0 + 7, x_0 + 14$, όπου σύμφωνα με το πόρισμα 3.4.5 το x_0 είναι η μοναδική λύση τής $2x \equiv 1(\mathrm{mod}\ 7)$ κατά μόδιο 7. Εφαρμόζοντας τον τύπο (3.12) θέτουμε

$$x_0 = 2^{\phi(7)-1} = 2^5 = 32 \equiv 4(\mathrm{mod}\,7).$$

Άρα οι λύσεις τής αρχικής είναι οι $4, 11, 18$ κατά μόδιο 21.

► **Συστήματα γραμμικών ισοτιμιών**. Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \ldots, a_k$, $b_1, \ldots, b_k$, υπό ποίες συνθήκες είναι το σύστημα των γραμμικών ισοτιμιών

$$\left\{ \begin{array}{c} a_1 x \equiv b_1\ (\mathrm{mod}\ m_1) \\ \vdots \\ a_k x \equiv b_k\ (\mathrm{mod}\ m_k) \end{array} \right\}$$

επιλύσιμο; Και πώς, πληρουμένων των εν λόγω συνθηκών, είναι δυνατόν να προσδιορισθεί επακριβώς το σύνολο λύσεων αυτού; Κατά την πορεία που θα ακολουθήσουμε προκειμένου να καταλήξουμε σε πλήρεις απαντήσεις σε αυτά τα ερωτήματα (μέσω τού θεωρηματος 3.4.16) θα χρησιμοποιήσουμε κατάλληλους *ισομορφισμούς δακτυλίων*.

3.4.7 Λήμμα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια, ώστε*

$$I_j + I_k = R,\ \forall\,(j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\ \ j \neq k,$$

τότε

$$R = I_j + \bigcap_{1 \leq k \leq n,\ k \neq j} I_k,\ \ \forall j \in \mathbb{N},\ \ 1 \leq j \leq n.$$

ΑΠΟΔΕΙΞΗ. Θα κάνουμε χρήση μαθηματικής επαγωγής ως προς τον n. Για $n = 2$ ο ισχυρισμός είναι προφανώς αληθής. Υποθέτουμε λοιπόν ότι είναι αληθής και για κάποιον $n = l \geq 2$ και εξετάζουμε την περίπτωση όπου $n = l + 1$. Επειδή ο R είναι δακτύλιος με μοναδιαίο στοιχείο, έχουμε[7] $R = RR$. Κατά συνέπειαν, για κάθε $j \in \mathbb{N}$, $1 \leq j \leq l + 1$,

$$R = RR = \left(I_j + \bigcap_{1 \leq k \leq l,\ k \neq j} I_k \right) (I_j + I_{l+1}) \subseteq I_j + \bigcap_{1 \leq k \leq l+1,\ k \neq j} I_k,$$

με τη δεύτερη ισότητα ισχύουσα λόγω επαγωγικής υποθέσεως και την επακόλουθη εγκλειστική σχέση απορρέουσα από την πρόταση 2.4.5 (ii). Επειδή όμως το δεξιό μέλος εμπεριέχεται στον R, έχουμε $R = I_j + \bigcap_{1 \leq k \leq l+1,\ k \neq j} I_k$. □

3.4.8 Θεώρημα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $I_1, I_2, \ldots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια ώστε*

$$I_j + I_k = R,\ \forall\,(j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\ \ j \neq k,$$

τότε έχουμε

$$\boxed{R/\bigcap_{j=1}^{n} I_j \cong (R/I_1) \times \cdots \times (R/I_n)\,.}$$

[7] Για δακτύλιους χωρίς μοναδιαίο κάτι τέτοιο δεν ισχύει εν γένει! Επί παραδείγματι, $(2\mathbb{Z})\,(2\mathbb{Z}) \subsetneqq (2\mathbb{Z})$.

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ. Για $n = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 3.3.19. Εάν υποτεθεί ότι $n \geq 3$ και ότι αυτός είναι αληθής για $n-1$ όρους, τότε μέσω μαθηματικής επαγωγής και εφαρμογής τού λήμματος 3.4.7 (για $j = n$) λαμβάνουμε

$$\begin{aligned} R/\bigcap_{j=1}^{n} I_j &= R/(\bigcap_{j=1}^{n-1} I_j \cap I_n) \underset{3.3.19}{\cong} \left(R/\bigcap_{j=1}^{n-1} I_j\right) \times R/I_n \\ &\underset{(\text{επαγ. υπ.})}{\cong} (R/I_1) \times \cdots \times (R/I_n)\,. \end{aligned}$$

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ. Αυτή η απόδειξη είναι καθαρώς *κατασκευαστική*. Για κάθε $j \in \{1, \ldots, n\}$ ορίζουμε την απεικόνιση

$$f : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$$

$$r \longmapsto f(r) := (\pi^R_{I_1}(r), .., \pi^R_{I_n}(r)) = (r + I_1, .., r + I_n)\,.$$

Η f είναι προφανώς ομομορφισμός δακτυλίων και $\mathrm{Ker}(f) = \bigcap_{j=1}^{n} I_j$. Θα δείξουμε ότι η f είναι και *επιρριπτική*. Έστω $\mathbf{y} = (y_1, \ldots, y_n) \in (R/I_1) \times \cdots \times (R/I_n)$. Επειδή κάθε $\pi^R_{I_j}$ είναι επιρριπτική απεικόνιση, υπάρχει $x_j \in R$, τέτοιο ώστε $\pi^R_{I_j}(x_j) = y_j$. Κατά το λήμμα 3.4.7,

$$\left[(\exists\, u_j \in I_j) \ \text{ και } \ (\exists\, v_j \in \bigcap_{1 \leq k \leq n,\ k \neq j} I_k) : u_j + v_j = 1_R\right].$$

Ως εκ τούτου, $v_j - 1_R \in I_j$ και $v_j \in I_k, \forall k \in \{1, \ldots, n\} \smallsetminus \{j\}$, απ' όπου έπεται ότι

$$\pi^R_{I_k}(v_j) = v_j + I_k = \begin{cases} 1_R + I_k, & \text{όταν } k = j, \\ I_k, & \text{όταν } k \neq j. \end{cases}$$

Συνεπώς,

$$\begin{aligned} f\left(\sum_{j=1}^{n} x_j v_j\right) &= \left(\pi^R_{I_1}(\sum_{j=1}^{n} x_j v_j), \ldots, \pi^R_{I_n}(\sum_{j=1}^{n} x_j v_j)\right) \\ &= \left(\pi^R_{I_1}(x_1), \ldots, \pi^R_{I_n}(x_n)\right) = \mathbf{y}, \end{aligned} \tag{3.14}$$

και η f είναι όντως επιρριπτική. Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3, ούτως ώστε να εισπράξουμε έναν «απτό» ισομορφισμό

$$\begin{aligned} R/\bigcap_{j=1}^{n} I_j &\xrightarrow{\cong} (R/I_1) \times \cdots \times (R/I_n) \\ r + \bigcap_{j=1}^{n} I_j &\longmapsto f(r) = (r + I_1, \ldots, r + I_n) \end{aligned} \tag{3.15}$$

μεταξύ των δύο θεωρηθέντων πηλικοδακτυλίων. □

3.4.9 Πόρισμα. *Έστω n ένας φυσικός αριθμός ≥ 2 και έστω*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ k \in \mathbb{N},$$

η παράσταση τού n ως γινομένου σαφώς διακεκριμένων πρώτων αριθμών $p_1, \ldots, p_k$, υψωμένων σε κατάλληλες δυνάμεις $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Τότε έχουμε

$$\boxed{\mathbb{Z}/\left(n\mathbb{Z}\right) \cong \mathbb{Z}/\left(p_1^{\alpha_1}\mathbb{Z}\right) \times \cdots \times \mathbb{Z}/\left(p_k^{\alpha_k}\mathbb{Z}\right).}$$

ΑΠΟΔΕΙΞΗ. Εάν $k = 1$, τούτο είναι προφανές. Έστω ότι $k \geq 2$ και ότι $I_j := p_j^{\alpha_j}\mathbb{Z}$ για κάθε $j \in \{1, \ldots, k\}$. Επειδή

$$\text{μκδ}(p_j^{\alpha_j}, p_l^{\alpha_l}) = 1,\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j, l \leq k,\ \ j \neq l,$$

υπάρχουν $\lambda, \mu \in \mathbb{Z}$, τέτοιοι ώστε $\lambda p_j^{\alpha_j} + \mu p_l^{\alpha_l} = 1$. Αυτό σημαίνει ότι για κάθε $x \in \mathbb{Z}$ έχουμε

$$x = x\lambda p_j^{\alpha_j} + x\mu p_l^{\alpha_l} \in I_j + I_l.$$

Άρα

$$I_j + I_l = \mathbb{Z},\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j, l \leq k,\ \ j \neq l.$$

Εν συνεχεία, θα αποδείξουμε την ισότητα

$$n\mathbb{Z} = \bigcap_{j=1}^{k} I_j.$$

Έστω τυχόν $x \in \langle n \rangle = n\mathbb{Z}$. Τότε $x = \lambda p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ για κάποιο $\lambda \in \mathbb{Z}$, οπότε

$$[x \in I_j,\ \ \forall j \in \{1, \ldots, k\}] \Longrightarrow x \in \bigcap_{j=1}^{k} I_j.$$

Και αντιστρόφως· εάν $x \in \bigcap_{j=1}^{k} I_j$, τότε $x = \mu_1 p_1^{\alpha_1} = \cdots = \mu_k p_k^{\alpha_k}$ για κάποια $\mu_1, \ldots, \mu_k \in \mathbb{Z}$. Συνεπώς,

$$\left.\begin{array}{r} p_j^{\alpha_j} \,\big|\, x, \quad \forall j \in \{1, \ldots, k\} \\ p_1, \ldots, p_k \\ \text{σαφώς διακεκριμένοι} \end{array}\right\} \Longrightarrow n = \prod_{j=1}^{k} p_j^{\alpha_j} \,\Bigg|\, x \Longrightarrow x \in \langle n \rangle = n\mathbb{Z}.$$

Αρκεί λοιπόν να εφαρμόσουμε το θεώρημα 3.4.8. $\square$

3.4.10 Πόρισμα. (Κινέζικο Θεώρημα ή Θεώρημα τού Νικομάχου τού Γερασηνού) *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, για τους οποίους ισχύει*

$$\text{μκδ}\,(m_j,m_l) = 1,\ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j,l \leq n,\ \ j \neq l,$$

το σύστημα των γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x \equiv b_1\,(\text{mod }\, m_1) \\ \vdots \\ x \equiv b_k\,(\text{mod }\, m_k) \end{array}\right\} \tag{3.16}$$

είναι επιλύσιμο. Μάλιστα, εάν το x_0 είναι μια λύση τού (3.16)*, τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο $m := \prod_{j=1}^{k} m_j$. *Ως εκ τούτου, το σύνολο των λύσεων τού συστήματος* (3.16) *είναι η κλάση υπολοίπων*[8]

$$x_0 + m\mathbb{Z}\ \ (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

Απόδειξη. Εάν για κάθε φυσικό αριθμό n και κάθε πρώτο αριθμό p ορίσουμε ως

$$\boldsymbol{\nu}_p\,(n) := \left\{\begin{array}{l} \text{τον εκθέτη τής μεγίστης δυνατής} \\ \text{δυνάμεως τού } p \text{ που διαιρεί τον } n \end{array}\right\} \in \mathbb{N}_0,$$

τότε, σύμφωνα με το πόρισμα 3.4.9,

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \prod_{p\ \text{πρώτος},\ p|m_1} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_1)}\mathbb{Z}) \times \cdots \times \prod_{p\ \text{πρώτος},\ p|m_k} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_k)}\mathbb{Z}),$$

και επειδή

$$m_j = \prod_{p\ \text{πρώτος},\ p|m_j} p^{\boldsymbol{\nu}_p(m_j)},\ \ \forall j \in \{1, \ldots, k\},$$

συμπεραίνουμε ότι

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}).$$

Εάν, μάλιστα, λάβει κανείς υπ' όψιν το 3.4.9 και τον (3.15), ο *τύπος ορισμού* αυτού τού ισομορφισμού είναι γνωστός, ήτοι ο

$$\mathbb{Z}/\,(m\mathbb{Z}) \ni \lambda + m\mathbb{Z} \longmapsto (\lambda + m_1\mathbb{Z}, \ldots, \lambda + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}). \tag{3.17}$$

[8] Εν προκειμένω, μπορούμε να *ταυτίζουμε* την $x_0 + m\mathbb{Z}\ \in \mathbb{Z}/\,(m\mathbb{Z})$ με την κλάση ισοτιμίας $[x_0]_m \in \mathbb{Z}_m$ μέσω τού ισομορφισμού (3.7).

Ιδιαιτέρως, το $(b_1 + m_1\mathbb{Z}, \ldots, b_k + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})$ διαθέτει ένα *μονοσημάντως ορισμένο αρχέτυπο*

$$x_0 + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$$

(κατά μόδιο m, όπου $x_0 \in \mathbb{Z}$), μέσω τού (3.17), οπότε έχουμε

$$x_0 + m_j\mathbb{Z} = b_j + m_j\mathbb{Z},\ \forall j \in \{1, ..., k\},$$

ήτοι k ισότητες που ισοδυναμούν με τη λύση τού συστήματος ισοτιμιών (3.16) κατά μόδιο m. □

3.4.11 Σημείωση. Για την εύρεση μιας λύσεως x_0 τού συστήματος (3.16) αρκεί, για κάθε δείκτη $j \in \{1, ..., k\}$, να προσδιορισθούν

$$u_j \in \langle m_j \rangle\,,\ \ v_j \in \langle m'_j \rangle = \bigcap_{1 \leq l \leq k,\ l \neq j} \langle m_l \rangle\,,$$

όπου

$$m'_j := \prod_{1 \leq l \leq k,\ l \neq j} m_l,$$

τέτοια ώστε $u_j + v_j = 1$, ή -ισοδυνάμως- $(y_j, z_j) \in \mathbb{Z}^2$, τέτοια ώστε

$$m_j y_j + m'_j z_j = 1,\ \forall j \in \{1, ..., k\}.$$

Επειδή όμως δεν θα χρειασθούμε ουσιαστικώς τα y_j, αρκεί να προσδιορίσουμε τη *μοναδική* κατά μόδιο m_j *λύση* $z_j \in \mathbb{Z}$ τής ισοτιμίας

$$m'_j z_j \equiv 1 (\mathrm{mod}\ m_j)$$

βάσει των όσων προαναφέραμε στη σημείωση 3.4.3. Εάν, επί παραδείγματι, εργασθούμε με το θεώρημα τού Euler, τότε μπορούμε να θέσουμε $z_j := {m'_j}^{\phi(m_j)-1}$. Από τα δεδομένα μας (βλ. (3.14), (3.15) και (3.17)) έπεται ότι το

$$\boxed{x_0 = \sum_{j=1}^{k} \frac{b_j z_j m}{m_j} = \sum_{j=1}^{k} b_j m'_j z_j = \sum_{j=1}^{k} b_j {m'_j}^{\phi(m_j)}} \tag{3.18}$$

-ανηγμένο κατά μόδιο m- είναι μια λύση τού συστήματος ισοτιμιών (3.16), ενώ κάθε άλλη λύση του προκύπτει κατόπιν αθροίσεως (σε αυτό) ενός ακεραίου πολλαπλασίου τού m.

3.4.12 Παράδειγμα. Το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x \equiv 1 \,(\mathrm{mod}\ 3) \\ x \equiv 2 \,(\mathrm{mod}\ 4) \\ x \equiv 3 \,(\mathrm{mod}\ 5) \end{array}\right\}$$

είναι η κλάση υπολοίπων $58 + 60\mathbb{Z}$ $(\in \mathbb{Z}/60\mathbb{Z})$, διότι (κατά τον τύπο (3.18))

$$\begin{aligned} x_0 &= \left(1 \cdot 20^{\phi(3)} + 2 \cdot 15^{\phi(4)} + 3 \cdot 12^{\phi(5)}\right) = 1 \cdot 20^2 + 2 \cdot 15^2 + 3 \cdot 12^4 \\ &= 1 \cdot 400 + 2 \cdot 225 + 3 \cdot 20\,736 = 63\,058 \equiv 58 (\mathrm{mod}\ 60). \end{aligned}$$

Τα δύο θεωρήματα 3.4.15 και 3.4.16 που ακολουθούν αποτελούν απλές γενικεύσεις τού 3.4.10. Μέσω αυτών το πρόβλημα τής επιλύσεως γραμμικών ισοτιμιών (με έναν άγνωστο) αντιμετωπίζεται σε *πλήρη γενικότητα*.

3.4.13 Λήμμα. *Εάν $m_1, m_2 \in \mathbb{N}$ και $b_1, b_2 \in \mathbb{Z}$, τότε υπάρχει ακέραιος αριθμός x με $x \equiv b_1 \,(\mathrm{mod}\ m_1)$ και $x \equiv b_2 \,(\mathrm{mod}\ m_2)$ εάν και μόνον εάν* μκδ $(m_1, m_2) \mid b_2 - b_1$.

ΑΠΟΔΕΙΞΗ. Εάν $x \in \mathbb{Z}$ με $x \equiv b_1 \,(\mathrm{mod}\ m_1)$ και $x \equiv b_2 \,(\mathrm{mod}\ m_2)$, τότε

$$\left.\begin{array}{c} m_1 \mid x - b_1 \\ m_2 \mid x - b_2 \end{array}\right\} \Longrightarrow \left.\begin{array}{c} \text{μκδ}\,(m_1, m_2) \mid x - b_1 \\ \text{μκδ}\,(m_1, m_2) \mid x - b_2 \end{array}\right\} \Longrightarrow \text{μκδ}\,(m_1, m_2) \mid x - b_1 - (x - b_2)\,.$$

Και αντιστρόφως· εάν $d :=$ μκδ(m_1, m_2) και $d \mid b_2 - b_1$, γράφοντας τον d ως ακέραιο γραμμικό συνδυασμό

$$d = k_1 m_1 + k_2 m_2, \quad k_1, k_2 \in \mathbb{Z},$$

και θέτοντας $\nu := \frac{k_1(b_2 - b_1)}{d}$, λαμβάνουμε

$$m_1 \nu \equiv (d - k_2 m_2)\, \frac{(b_2 - b_1)}{d} \equiv b_2 - b_1 \,(\mathrm{mod}\, m_2)\,,$$

οπότε για τον ακέραιο αριθμό $x := b_1 + m_1 \nu$ ισχύουν οι ισοτιμίες $x \equiv b_1 (\mathrm{mod}\ m_1)$ και $x \equiv b_1 + (b_2 - b_1) \equiv b_2 (\mathrm{mod}\ m_2)$. □

3.4.14 Λήμμα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ έχουμε*

$$\text{μκδ}\,(\text{εκπ}\,(m_1, \ldots, m_{k-1})\,, m_k) = \text{εκπ}\,(\text{μκδ}\,(m_1, m_k)\,, \ldots, \text{μκδ}\,(m_{k-1}, m_k))$$

3.4.15 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{\begin{array}{c} x \equiv b_1 \,(\mathrm{mod}\ m_1) \\ \vdots \\ x \equiv b_k \,(\mathrm{mod}\ m_k) \end{array}\right\} \tag{3.19}$$

είναι επιλύσιμο εάν και μόνον εάν

$$\text{μκδ}\,(m_j, m_l) \mid b_j - b_l,\ \ \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j,l \leq k,\ \ j \neq l. \tag{3.20}$$

Μάλιστα, εάν το x_0 *είναι μια λύση τού* (3.19), *τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο

$$m := \text{εκπ}\,(m_1, m_2, ..., m_k)\,.$$

Ως εκ τούτου, όταν ικανοποιούνται οι συνθήκες (3.20)*, το σύνολο των λύσεων τού συστήματος* (3.19) *είναι η κλάση υπολοίπων*

$$x_0 + m\mathbb{Z}\ \ (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

ΑΠΟΔΕΙΞΗ. (i) Έστω x_0 είναι μια λύση τού (3.19). Τότε για κάθε $j, l \in \{1, \ldots, k\}$ με $j \neq l$ έχουμε

$$\left.\begin{array}{r} x_0 \equiv b_j\,(\text{mod }m_j) \\ x_0 \equiv b_l\,(\text{mod }m_l) \end{array}\right\} \Longrightarrow \left.\begin{array}{c} m_j \mid x_0 - b_j \\ m_l \mid x_0 - b_l \end{array}\right\} \Longrightarrow \left.\begin{array}{c} \text{μκδ}\,(m_j, m_l) \mid x_0 - b_j \\ \text{μκδ}\,(m_j, m_l) \mid x_0 - b_l \end{array}\right\} \Longrightarrow (3.20).$$

Και αντιστρόφως· ας υποθέσουμε την ισχύ των συνθηκών (3.20).

Εργαζόμενοι επαγωγικώς θα κατασκευάσουμε για κάθε $j \in \{1, \ldots, k\}$ έναν ακέραιο αριθμό y_j, ούτως ώστε να ισχύουν οι ισοτιμίες

$$\left\{\begin{array}{c} y_j \equiv b_1\,(\text{mod }m_1) \\ \vdots \\ y_j \equiv b_j\,(\text{mod }m_j) \end{array}\right\}.$$

Κατ' αρχάς ορίζουμε ως y_1 έναν εκπρόσωπο τής κλάσεως υπολοίπων $[b_1]_{m_1}$. Εάν $j \in \{1, \ldots, k-1\}$ και υποθέσουμε ότι οι ακέραιοι $y_1, \ldots, y_j$ έχουν ήδη ορισθεί, κατασκευάζουμε κατάλληλο ακέραιο y_{j+1} ως ακολούθως: Επειδή

$$y_j \equiv b_l\,(\text{mod }m_l)\,,\quad \forall l \in \{1, \ldots, j\},$$

έχουμε

$$[m_l \mid y_j - b_l,\ \forall l \in \{1, \ldots, j\}] \Longrightarrow [\text{μκδ}\,(m_l, m_{j+1}) \mid y_j - b_l,\ \forall l \in \{1, \ldots, j\}]\,.$$

Εξ υποθέσεως,

$$\text{μκδ}\,(m_l, m_{j+1}) \mid b_l - b_{j+1},\ \forall l \in \{1, \ldots, j\}.$$

Άρα

$$\text{μκδ}\,(m_l, m_{j+1}) \mid (y_j - b_l) + (b_l - b_{j+1}) = y_j - b_{j+1},\ \forall l \in \{1, \ldots, j\}$$

και, ως εκ τούτου,

$$\text{εκπ}\left(\text{μκδ}\left(m_1, m_{j+1}\right), \ldots, \text{μκδ}\left(m_j, m_{j+1}\right)\right) \mid y_j - b_{j+1}.$$

Εφαρμόζοντας λοιπόν το λήμμα 3.4.14 συμπεραίνουμε ότι

$$\text{μκδ}\left(\text{εκπ}\left(m_1, \ldots, m_j\right), m_{j+1}\right) \mid y_j - b_{j+1}.$$

Κατά συνέπειαν, βάσει τού λήμματος 3.4.13 υπάρχει ένας $y_{j+1} \in \mathbb{Z}$, τέτοιος ώστε

$$y_{j+1} \equiv y_j \left(\text{mod } \text{εκπ}\left(m_1, \ldots, m_j\right)\right) \qquad y_{j+1} \equiv b_{j+1} \left(\text{mod } m_{j+1}\right),$$

οπότε

$$\left[m_l \mid \text{εκπ}\left(m_1, .., m_j\right), \forall l \in \{1, .., j\}\right] \Longrightarrow y_{j+1} \equiv y_j \equiv b_l \left(\text{mod } m_l\right), \forall l \in \{1, .., j\}.$$

(ii) Έστω τώρα $m := \text{εκπ}(m_1, m_2, ..., m_k)$ και έστω x_0 ο (μοναδικός) εκπρόσωπος τής κλάσεως υπολοίπων $[y_k]_m$ με $0 \leq x_0 < m$. Εάν ο x είναι ένας ακέραιος αριθμός, ο οποίος πληροί τις k ισοτιμίες (3.19), τότε έχουμε

$$\left[x \equiv b_\ell \equiv x_0 \left(\text{mod } m_\ell\right), \forall \ell \in \{1, \ldots, k\}\right],$$

οπότε

$$\left[m_\ell \mid x_0 - x,\ \forall \ell \in \{1, \ldots, k\}\right] \Longrightarrow m \mid x_0 - x \Longrightarrow x_0 - x \in m\mathbb{Z}.$$

Και αντιστρόφως· εάν $x \in \mathbb{Z}$ και $x \equiv x_0 \left(\text{mod } m\right)$, τότε έχουμε προφανώς για κάθε $\ell \in \{1, \ldots, k\}$: $x \equiv b_\ell \equiv x_0 \left(\text{mod } m_\ell\right)$. □

3.4.16 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \ldots, a_k,\ b_1, \ldots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{\begin{array}{c} a_1 x \equiv b_1 \left(\text{mod } m_1\right) \\ \vdots \\ a_k x \equiv b_k \left(\text{mod } m_k\right) \end{array}\right\} \tag{3.21}$$

δεν είναι επιλύσιμο εάν δεν ικανοποιούνται ταυτοχρόνως οι συνθήκες

$$\text{μκδ}\left(a_j, m_j\right) \mid b_j, \quad \forall j \in \{1, ..., k\}. \tag{3.22}$$

Από την άλλη μεριά, όταν οι συνθήκες (3.22) ικανοποιούνται, το σύνολο των λύσεων τού συστήματος (3.21) ταυτίζεται με το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x \equiv c_1 \left(\text{mod } m_1^\star\right) \\ \vdots \\ x \equiv c_k \left(\text{mod } m_k^\star\right) \end{array}\right\} \tag{3.23}$$

όπου

$$c_j := \left(a_j^{\star}\right)^{\phi\left(m_j^{\star}\right)-1} \, b_j^{\star}$$

και

$$a_j^{\star} := \frac{a_j}{\text{μκδ}\,(a_j, m_j)}, \;\; b_j^{\star} := \frac{b_j}{\text{μκδ}\,(a_j, m_j)}, \;\; m_j^{\star} := \frac{m_j}{\text{μκδ}\,(a_j, m_j)},$$

για κάθε $j \in \{1, ..., k\}$ και ϕ η συνάρτηση τού Euler.

Απόδειξη. Για να υπάρχουν κοινές λύσεις τού συστήματος (3.21) θα πρέπει τουλάχιστον καθεμιά των ισοτιμιών του να είναι επιλύσιμη από μόνη της. Τούτο σημαίνει (επί τη βάσει τής προτάσεως 3.4.1) ότι μκδ$(a_j, m_j) \mid b_j$ για κάθε δείκτη $j \in \{1, ..., k\}$. Από την άλλη μεριά, εάν οι συνθήκες (3.22) ικανοποιούνται, εφαρμόζουμε το πόρισμα 3.4.5 για κάθε μία εκ των αρχικών ισοτιμιών και συμπεραίνουμε ότι το (3.21) ισοδυναμεί με το σύστημα

$$\left\{\begin{array}{c} a_1^{\star}x \equiv b_1^{\star} \,(\text{mod } m_1^{\star}) \\ \vdots \\ a_k^{\star}x \equiv b_k^{\star} \,(\text{mod } m_k^{\star}) \end{array}\right\} \tag{3.24}$$

Επειδή μκδ$(a_j^{\star}, m_j^{\star}) = 1$, η γραμμική ισοτιμία $a_j^{\star}x \equiv b_j^{\star} \left(\text{mod } m_j^{\star}\right)$ διαθέτει μοναδική λύση κατά μόδιο $m_j^{\star}$, ήτοι την $x \equiv c_j (\text{mod } m_j^{\star})$ (βλ. 3.4.3), οπότε το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών (3.24) ταυτίζεται με το σύνολο των λύσεων τού συστήματος (3.23). □

3.4.17 Παρατήρηση. Προφανώς, το πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.21) ανάγεται στο πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.23), ήτοι ενός συστήματος τού τύπου (3.19), οπότε αντιμετωπίζεται βάσει των όσων ελέχθησαν στο θεώρημα 3.4.15.

3.4.18 Παράδειγμα. Ας θεωρήσουμε το ακόλουθο σύστημα τριών γραμμικών ισοτιμιών:

$$\left\{\begin{array}{l} 2x \equiv 4 \,(\text{mod } 8) \\ 6x \equiv 12 \,(\text{mod } 9) \\ x \equiv 14 \,(\text{mod } 12) \end{array}\right\}.$$

Επειδή μκδ$(2, 8) = 2 \mid 4$, μκδ$(6, 9) = 3 \mid 12$ και μκδ$(1, 12) = 1 \mid 14$, αυτό είναι ισοδύναμο με το

$$\left\{\begin{array}{l} x \equiv 2 \,(\text{mod } 4) \\ 2x \equiv 4 \,(\text{mod } 3) \\ x \equiv 14 \,(\text{mod } 12) \end{array}\right\}.$$

Η δεύτερη ισοτιμία έχει ως λύση της την κλάση υπολοίπων $2 + 3\mathbb{Z}$ $(\in \mathbb{Z}/3\mathbb{Z})$, διότι $2^{\phi(3)-1} \cdot 4 = 8 \equiv 2 \,(\mathrm{mod}\ 3)$. Ως εκ τούτου, βάσει τού θεωρήματος 3.4.16 το ανωτέρω σύστημα είναι ισοδύναμο με το

$$\left\{ \begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 4) \\ x \equiv 2 \,(\mathrm{mod}\ 3) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\},$$

το οποίο διαθέτει μοναδική λύση κατά μόδιο εκπ$(4, 3, 12) = 12$, αφού

$$\text{μκδ}\,(4,3) = 1 \mid 4-3,\ \ \text{μκδ}\,(12,3) = 3 \mid 14-2,\ \ \text{μκδ}\,(12,4) = 4 \mid 14-2$$

(βλ. θεώρημα 3.4.15). Επειδή έχουμε μκδ$(4, 3) = 1$, η μοναδική λύση x_0 (κατά μόδιο $4 \cdot 3 = 12$) των δύο πρώτων ισοτιμιών προσδιορίζεται μέσω τού θεωρήματος 3.4.10. Πράγματι· κατά τον τύπο (3.18),

$$x_0 = 2 \cdot 3^{\phi(4)} + 2 \cdot 4^{\phi(3)} = 50 \equiv 2 \,(\mathrm{mod}\ 12)\,,$$

λύση, η οποία επαληθεύει (κατ' ανάγκην!) *και* την τρίτη εκ των ανωτέρω ισοτιμιών (βλ. θεώρημα 3.4.15).

3.5 ΣΩΜΑ ΚΛΑΣΜΑΤΩΝ ΑΚΕΡΑΙΑΣ ΠΕΡΙΟΧΗΣ

Τα σώματα, από τον ίδιο τους τον ορισμό, χαίρουν λίαν ευάρεστων ιδιοτήτων, όπως, επί παραδείγματι, είναι η ύπαρξη αντιστρόφου για κάθε μη μηδενικό στοιχείο τους. Αντικείμενο τής παρούσας ενότητας είναι η απόδειξη τού ότι *κάθε* ακεραία περιοχή μπορεί να εμφυτευθεί *κατά τρόπο φυσικό* σε ένα σώμα. Αυτή επιτυγχάνεται μέσω τής γενικεύσεως τής γνωστής μεθόδου κατασκευής των ρητών αριθμών από τους ακεραίους.

3.5.1 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Επί τού $R \times (R \smallsetminus \{0_R\})$ ορίζουμε μια διμελή σχέση "$\sim$" ως ακολούθως:

$$\boxed{(a,b) \sim (c,d) \underset{\text{ορσ}}{\Longleftrightarrow} ad = bc.}$$

3.5.2 Πρόταση. *Η "$\sim$" αποτελεί μια σχέση ισοδυναμίας.*

ΑΠΟΔΕΙΞΗ. Η "$\sim$" είναι *ανακλαστική*, διότι

$$ab = ba \Rightarrow (a,b) \sim (a,b)\,,\ \ \forall (a,b) \in R \times (R \smallsetminus \{0_R\})\,,$$

συμμετρική, διότι για οιαδήποτε ζεύγη $(a,b), (c,d) \in R \times (R \smallsetminus \{0_R\})$ έχουμε

$$(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)\,,$$

και, τέλος, *μεταβατική*, αφού για οιαδήποτε $(a,b),(a',b'),(a'',b'') \in R\times(R\smallsetminus\{0_R\})$ με

$$(a,b)\sim(a',b') \text{ και } (a',b')\sim(a'',b'')$$

έχουμε $ab'=ba'$ και $a'b''=b'a''$, οπότε

$$ab''b'=ab'b''=ba'b''=bb'a''=ba''b',$$

και, ως εκ τούτου,

$$\left.\begin{array}{r}(ab''-ba'')b'=0_R\\ b'\neq 0_R\end{array}\right\}\Longrightarrow ab''=ba''\Longrightarrow (a,b)\sim(a'',b'')$$

(με την πρώτη εκ των ανωτέρω συνεπαγωγών οφειλόμενη στο ότι ο δακτύλιος R είναι ακεραία περιοχή). □

3.5.3 Ορισμός. Έστω R τυχούσα ακεραία περιοχή. Ως

$$\boxed{\mathbf{Fr}(R):=(R\times(R\smallsetminus\{0_R\}))\,/\sim}$$

συμβολίζουμε το σύνολο κλάσεων ισοδυναμίας ως προς την “$\sim$”. Το **κλάσμα** ενός $a\in R$ «διηρημένου» διά ενός $b\in R\smallsetminus\{0_R\}$ είναι η κλάση ισοδυναμίας

$$\frac{a}{b}:=[(a,b)]:=\{\,(x,y)\in R\times(R\smallsetminus\{0_R\})\mid (x,y)\sim(a,b)\}.$$

Το $\mathbf{Fr}(R)$ επιδέχεται πρόσθεση και πολλαπλασιασμό:

$$\left\{\begin{array}{lcl}\dfrac{a}{b}+\dfrac{c}{d} & := & \dfrac{ad+cb}{bd},\\[2ex] \dfrac{a}{b}\cdot\dfrac{c}{d} & := & \dfrac{ac}{bd}.\end{array}\right.$$

3.5.4 Πρόταση. *Οι εν λόγω πράξεις είναι καλώς ορισμένες.*

ΑΠΟΔΕΙΞΗ. Εάν για κάποια ζεύγη $(a,b)\,,(a',b')$ και $(c,d)\,,(c',d')\in R\times(R\smallsetminus\{0_R\})$ έχουμε $[(a,b)]=[(a',b')]$ και $[(c,d)]=[(c',d')]$, τότε

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'} \text{ και } \frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}.$$

Πράγματι· επειδή εξ υποθέσεως

$$\left.\begin{array}{r}(a,b)\sim(a',b')\\ (c,d)\sim(c',d')\end{array}\right\}\Longrightarrow \left.\begin{array}{r}ab'=ba'\\ cd'=dc'\end{array}\right\}\Longrightarrow \left.\begin{array}{r}ab'dd'=ba'dd'\\ cd'bb'=dc'bb'\end{array}\right\},$$

(κατόπιν προσθέσεως κατά μέλη) έπεται ότι

$$ab'dd' + cd'bb' = ba'dd' + dc'bb' \Longrightarrow (ad+cb)\, b'd' = (a'd' + c'b')\, bd,$$

ήτοι ότι

$$\tfrac{ad+cb}{bd} = \tfrac{a'd'+c'b'}{b'd'} \Longrightarrow \tfrac{a}{b} + \tfrac{c}{d} = \tfrac{a'}{b'} + \tfrac{c'}{d'}.$$

Εξάλλου, πολλαπλασιασμός κατά μέλη μάς οδηγεί στην ισότητα $ab'cd' = ba'dc'$, απ' όπου λαμβάνουμε

$$(ac)\,(b'd') = (bd)\,(a'c') \Longrightarrow \tfrac{ac}{bd} = \tfrac{a'c'}{b'd'},$$

ήτοι $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$. □

3.5.5 Θεώρημα. *Το σύνολο* $\mathbf{Fr}(R)$ *των κλασμάτων μιας ακεραίας περιοχής* R *αποτελεί ένα σώμα ως προς τις ως άνω ορισθείσες πράξεις προσθέσεως και πολλαπλασιασμού.* (*Γι' αυτόν τον λόγο το* $\mathbf{Fr}(R)$ *ονομάζεται* ***σώμα κλασμάτων*** *τής ακεραίας περιοχής* R.)

ΑΠΟΔΕΙΞΗ. (i) Η "+" είναι *προσεταιριστική και μεταθετική*, διότι

$$\begin{aligned}\left(\tfrac{a}{b} + \tfrac{c}{d}\right) + \tfrac{e}{f} &= \tfrac{ad+cb}{bd} + \tfrac{e}{f} = \tfrac{adf+cbf+ebd}{bdf} \\ &= \tfrac{adf+(cf+ed)b}{bdf} = \tfrac{a}{b} + \tfrac{cf+ed}{df} = \tfrac{a}{b} + \left(\tfrac{c}{d} + \tfrac{e}{f}\right)\end{aligned}$$

και $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} = \frac{cb+ad}{bd} = \frac{c}{d} + \frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$.
(ii) Το *μηδενικό στοιχείο* (= ουδέτερο στοιχείο ως προς την "+") τού $\mathbf{Fr}(R)$ είναι το[9] $0_{\mathbf{Fr}(R)} := \frac{0_R}{1_R}$, διότι για κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\tfrac{a}{b} + \tfrac{0_R}{1_R} = \tfrac{(a \cdot 1_R)+(b \cdot 0_R)}{b \cdot 1_R} = \tfrac{a}{b} = \tfrac{(b_R \cdot b)+(1_R \cdot a)}{1_R \cdot b} = \tfrac{0_R}{1_R} + \tfrac{a}{b}.$$

(iii) Κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ έχει το κλάσμα $\frac{-a}{b}$ ως *αντίθετό του* ως προς την "+", καθότι

$$\tfrac{a}{b} + \tfrac{-a}{b} = \tfrac{ab+(-a)b}{b^2} = \tfrac{(a+(-a))b}{b^2} = \tfrac{a+(-a)}{b} = \tfrac{0_R}{b} = \tfrac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}$$

και

$$\tfrac{-a}{b} + \tfrac{a}{b} = \tfrac{(-a)b+ab}{b^2} = \tfrac{((-a)+a)b}{b^2} = \tfrac{(-a)+a}{b} = \tfrac{0_R}{b} = \tfrac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}.$$

(iv) Η "·" είναι *προσεταιριστική και μεταθετική*, διότι

$$\left(\tfrac{a}{b} \cdot \tfrac{c}{d}\right) \cdot \tfrac{e}{f} = \left(\tfrac{ac}{bd}\right) \cdot \tfrac{e}{f} = \tfrac{(ac)e}{(bd)f} = \tfrac{a(ce)}{b(df)} = \tfrac{a}{b} \cdot \left(\tfrac{ce}{df}\right) = \tfrac{a}{b} \cdot \left(\tfrac{c}{d} \cdot \tfrac{e}{f}\right)$$

[9]Σημειωτέον ότι *για κάθε* $b \in R \smallsetminus \{0_R\}$ έχουμε $\frac{0_R}{b} = \frac{0_R}{1_R}$.

και $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$ για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$.

(v) Η "$\cdot$" είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "$+$". Επειδή η "$\cdot$" είναι μεταθετική, αρκεί προς τούτο να ελεγχθεί η επιμεριστικότητα μόνον εκ δεξιών. Για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned}\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} &= \left(\frac{ad+cb}{bd}\right) \cdot \frac{e}{f} = \frac{(ad+cb)e}{(bd)f} = \frac{ade+cbe}{bdf} = \frac{ade}{bdf} + \frac{cbe}{bdf} \\ &= \frac{ae}{bf} + \frac{ce}{df} = \left(\frac{a}{b} \cdot \frac{e}{f}\right) + \left(\frac{c}{d} \cdot \frac{e}{f}\right).\end{aligned}$$

(vi) Το $1_{\mathbf{Fr}(R)} := \frac{1_R}{1_R}$ είναι *μοναδιαίο στοιχείο*[10] (= ουδέτερο στοιχείο ως προς την "$\cdot$") τού $\mathbf{Fr}(R)$, διότι για κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ ισχύουν οι ισότητες

$$\frac{a}{b} \cdot 1_{\mathbf{Fr}(R)} = \frac{a}{b} \cdot \frac{1_R}{1_R} = \frac{a \cdot 1_R}{b \cdot 1_R} = \frac{a}{b} = \frac{1_R \cdot a}{1_R \cdot b} = \frac{1_R}{1_R} \cdot \frac{a}{b} = 1_{\mathbf{Fr}(R)} \cdot \frac{a}{b}.$$

(vii) Εκ των (i)-(vi) συνάγουμε ότι η τριάδα $(\mathbf{Fr}(R), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Επομένως, για να αποδείξουμε, επιπροσθέτως, ότι αυτός ο δακτύλιος είναι και *σώμα*, αρκεί να αποδείξουμε ότι οιοδήποτε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\}$ είναι αντιστρέψιμο. Επειδή από τη συνθήκη $\frac{a}{b} \neq \frac{0_R}{1_R}$ προκύπτει ότι

$$a = a \cdot 1_R \neq 0_R \cdot b = 0_R \Longrightarrow \frac{b}{a} \in \mathbf{Fr}(R),$$

εκ των ισοτήτων

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1_R}{1_R} = 1_{\mathbf{Fr}(R)} = \frac{ba}{ba} = \frac{ba}{ab} = \frac{b}{a} \cdot \frac{a}{b}$$

συμπεραίνουμε ότι το $\frac{b}{a}$ είναι *το αντίστροφο* τού $\frac{a}{b}$. □

3.5.6 Παραδείγματα. (i) Προφανώς, $\mathbf{Fr}(\mathbb{Z}) = \mathbb{Q}$.

(ii) Εάν το K είναι ένα σώμα, το

$$\boxed{K(\mathsf{X}) := \mathbf{Fr}(K[\mathsf{X}])}$$

καλείται **σώμα των ρητών συναρτήσεων** ή **των ρητών εκφράσεων μιας απροσδιορίστου** X **υπεράνω τού** K. Κατ' αναλογίαν, το

$$\boxed{K(\mathsf{X}_1, \ldots, \mathsf{X}_n) := \mathbf{Fr}(K[\mathsf{X}_1, \ldots, \mathsf{X}_n])}$$

είναι το **σώμα των ρητών συναρτήσεων** n **απροσδιορίστων** $\mathsf{X}_1, .., \mathsf{X}_n$ **υπεράνω τού** K.

[10] Σημειωτέον ότι *για κάθε* $c \in R \smallsetminus \{0_R\}$ έχουμε $\frac{c}{c} = 1_{\mathbf{Fr}(R)}$.

(iii) Εντός τής ακεραίας περιοχής $\mathbb{C}[\![\mathsf{Z}]\!]$ των επίτυπων δυναμοσειρών μιας μιγαδικής απροσδιορίστου Z (ήτοι μιας απροσδιορίστου Z υπεράνω τού $\mathbb{C}$) ορίζεται η υποπεριοχή

$$\mathbb{C}\{\mathsf{Z}\} := \left\{ \sum_{i=0}^{\infty} a_i \mathsf{Z}^i \in \mathbb{C}[\![\mathsf{Z}]\!] \,\middle|\, \sum_{i=0}^{\infty} a_i z^i \text{ συγκλίνουσα για κάθε } z \in \mathbb{C} \right\}.$$

Ως γνωστόν[11], $\mathbb{C}\{\mathsf{Z}\} = \mathcal{O}(\mathbb{C})$, όπου

$$\boxed{\mathcal{O}(\mathbb{C}) := \{\text{συναρτήσεις } f : \mathbb{C} \longrightarrow \mathbb{C} \,|\, f \text{ ολόμορφη}\}}$$

η ακεραία περιοχή των λεγομένων **ακεραίων συναρτήσεων** μιας μιγαδικής μεταβλητής. Το σώμα κλασμάτων της

$$\boxed{\mathcal{M}(\mathbb{C}) := \mathbf{Fr}(\mathcal{O}(\mathbb{C}))}$$

καλείται **σώμα των μερομόρφων συναρτήσεων** επί τού $\mathbb{C}$ (και τα στοιχεία του **μερόμορφες συναρτήσεις** επί τού $\mathbb{C}$, τις οποίες συναντούμε συχνά στο μάθημα τής Μιγαδικής Αναλύσεως).

(iv) Έστω R μια ακεραία περιοχή. Τότε

$$\boxed{\mathbf{Fr}(R\,[\mathsf{X}]) = \mathbf{Fr}(R)(\mathsf{X}) \ (:= \mathbf{Fr}(\mathbf{Fr}(R)[\mathsf{X}])),}$$

διότι έχουμε αφ' ενός μεν

$$\mathbf{Fr}(R\,[\mathsf{X}]) = \left\{ \frac{a_0 + a_1\mathsf{X} + \cdots + a_n\mathsf{X}^n}{b_0 + b_1\mathsf{X} + \cdots + b_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m, n \in \mathbb{N}_0, a_0, \ldots, a_n, b_0, \ldots, b_m \in R \\ \text{με } \ b_j \neq 0_R \text{ για κάποιον } \ j \in \{0, \ldots, m\} \end{array} \right\},$$

αφ' ετέρου δε

$$\begin{aligned}
\mathbf{Fr}(R)(\mathsf{X}) &= \left\{ \tfrac{r_0 + r_1\mathsf{X} + \cdots + r_n\mathsf{X}^n}{s_0 + s_1\mathsf{X} + \cdots + s_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m, n \in \mathbb{N}_0, r_0, \ldots, r_n, s_0, \ldots, s_m \in \mathbf{Fr}(R) \\ \text{με } \ s_j \neq 0_{\mathbf{Fr}(R)} \text{ για κάποιον } \ j \in \{0, \ldots, m\} \end{array} \right\} \\
&= \left\{ \frac{\frac{a_0}{b_0} + \left(\frac{a_1}{b_1}\right)\mathsf{X} + \cdots + \left(\frac{a_n}{b_n}\right)\mathsf{X}^n}{\frac{c_0}{d_0} + \left(\frac{c_1}{d_1}\right)\mathsf{X} + \cdots + \left(\frac{c_m}{d_m}\right)\mathsf{X}^m} \,\middle|\, \begin{array}{c} r_i = \frac{a_i}{b_i},\ s_j = \frac{c_j}{d_j}, \\ \text{όπου } (a_i, b_i), (c_j, d_j) \in R \times (R \smallsetminus \{0_R\}), \\ \forall (i, j) \in \{0, \ldots, n\} \times \{0, \ldots, m\} \end{array} \right\} \\
&= \mathbf{Fr}(R\,[\mathsf{X}]),
\end{aligned}$$

με την τελευταία ισότητα προκύπτουσα ύστερα από απαλοιφή παρονομαστών.

(v) Εάν το K είναι ένα σώμα, τότε το σώμα των κλασμάτων τής ακεραίας περιοχής

[11] Κάθε *ολόμορφη συνάρτηση* $f : \mathbb{C} \longrightarrow \mathbb{C}$ (ήτοι κάθε συνάρτηση $f : \mathbb{C} \longrightarrow \mathbb{C}$ διαθέτουσα μιγαδική παράγωγο σε κάθε σημείο τού $\mathbb{C}$) είναι *παραστάσιμη ως συγκλίνουσα δυναμοσειρά*.

$K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας απροσδιορίστου X με συντελεστές ειλημμένους από το K συμβολίζεται συντόμως ως ακολούθως:

$$\boxed{K(\!(\mathsf{X})\!) := \mathbf{Fr}(K[\![\mathsf{X}]\!]).}$$

Σημειωτέον ότι

$$\boxed{K(\!(\mathsf{X})\!) = \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]}$$

(βλ. άσκηση **1-43**). Πράγματι· για τυχόν στοιχείο

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} \in K(\!(\mathsf{X})\!)$$

παρατηρούμε τα εξής: Εάν $b_0 \neq 0_K$, τότε $\sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]^{\times}$ (βλ. 1.3.9 (iii)) και

$$\frac{\sum_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum_{i=0}^{\infty} b_i \mathsf{X}^i} = \left(\sum_{i=0}^{\infty} a_i \mathsf{X}^i\right)\left(\sum_{i=0}^{\infty} b_i \mathsf{X}^i\right)^{-1} \in K[\![\mathsf{X}]\!].$$

Εάν $b_0 = 0_K$, τότε $l := \mathrm{ord}(\sum_{i=0}^{\infty} b_i \mathsf{X}^i) \geq 1$ (βλ. 1.3.4), οπότε

$$b_0 = \cdots = b_{l-1} = 0_K,\ b_l \neq 0_K \Rightarrow \sum_{i=l}^{\infty} b_i \mathsf{X}^{i-l} \in K[\![\mathsf{X}]\!]^{\times}$$

και

$$\frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=0}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^i} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i}{\mathsf{X}^l\left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)} = \frac{\sum\limits_{i=0}^{\infty} a_i \mathsf{X}^i \left(\sum\limits_{i=l}^{\infty} b_i \mathsf{X}^{i-l}\right)^{-1}}{\mathsf{X}^l}.$$

Κατά συνέπειαν,

$$\begin{aligned} K(\!(\mathsf{X})\!) &= \left\{ \frac{\sum_{i=0}^{\infty} c_i \mathsf{X}^i}{\mathsf{X}^l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \left\{ \sum\limits_{i=0}^{l-1} c_i \mathsf{X}^{i-l} + \sum\limits_{i=l}^{\infty} c_i \mathsf{X}^{i-l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]. \end{aligned}$$

3.5.7 Πρόταση. *Κάθε ακεραία περιοχή εμφυτεύεται στο σώμα των κλασμάτων της.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα ακεραία περιοχή. Τότε ο ομομορφισμός

$$j : R \longrightarrow \mathbf{Fr}(R), \quad a \longmapsto j(a) := \tfrac{a}{1_R}, \tag{3.25}$$

είναι ένας μονομορφισμός, διότι έχει το $\{\, a \in R \mid \frac{a}{1_R} = \frac{0_R}{1_R}\} = \{0_R\}$ ως πυρήνα του (βλ. πρόταση 3.1.15). □

3.5.8 Πρόταση. (“**Καθολική ιδιότητα**” **τού** $\mathbf{Fr}(R)$.) *Έστω* R *μια ακεραία περιοχή. Τότε για κάθε μονομορφισμό* $f : R \longrightarrow K$, *όπου* K *ένα σώμα, υφίσταται ένας και μόνον μονομορφισμός σωμάτων* $\eta : \mathbf{Fr}(R) \longrightarrow K$ *ο οποίος καθιστά το διάγραμμα*

$$\begin{tikzcd} R \arrow[d, "j"'] \arrow[dr, "f"] & \\ \mathbf{Fr}(R) \arrow[r, "\eta"'] \arrow[ur, phantom, "\circlearrowleft"] & K \end{tikzcd}$$

μεταθετικό (*ήτοι* $f = \eta \circ j$), *όπου* j *ο μονομορφισμός* (3.25).

ΑΠΟΔΕΙΞΗ. Ορίζουμε την $\eta : \mathbf{Fr}(R) \longrightarrow K$ μέσω τού τύπου

$$\eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1}, \ \ \forall \tfrac{a}{b} \in \mathbf{Fr}(R).$$

Η η είναι *καλώς ορισμένη* απεικόνιση, διότι για $\frac{a}{b}, \frac{a'}{b'} \in \mathbf{Fr}(R)$ με $\frac{a}{b} = \frac{a'}{b'}$ έχουμε

$$ab' = ba' \Rightarrow f(a)f(b') = f(ab') = f(ba') = f(b)f(a'),$$

οπότε

$$f(b), f(b') \in \mathbf{Fr}(R)^{\times} \Rightarrow \eta(\tfrac{a}{b}) := f(a)\, f(b)^{-1} = f(a')\, f(b')^{-1} =: \eta(\tfrac{a'}{b'}).$$

Η η είναι *ομομορφισμός*, καθότι για οιαδήποτε $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \eta(\tfrac{a}{b} + \tfrac{c}{d}) &= \eta(\tfrac{ad+cb}{bd}) = f(ad+cb)\, f(bd)^{-1} \\ &= (f(a)f(d) + f(c)f(b))\, f(b)f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)\, f(d)^{-1} = \eta(\tfrac{a}{b}) + \eta(\tfrac{c}{d}) \end{aligned}$$

και

$$\begin{aligned} \eta(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= \eta(\tfrac{ac}{bd}) = f(ac)\, f(bd)^{-1} \\ &= \left(f(a)f(b)^{-1}\right)\left(f(c)\, f(d)^{-1}\right) \\ &= \eta(\tfrac{a}{b})\eta(\tfrac{c}{d}). \end{aligned}$$

Η η είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ με $\eta(\frac{a}{b}) = \eta(\frac{c}{d})$, τότε

$$f(a)\, f(b)^{-1} = f(c)\, f(d)^{-1} \Rightarrow f(a)\, f(d) = f(b)\, f(c),$$

ήτοι

$$f(ad) = f(bc) \underset{[f \text{ ένριψη}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

απ' όπου έπεται ότι η η είναι πράγματι ένας *μονομορφισμός*. Προφανώς,

$$(\eta \circ j)(a) = \eta(j(a)) = \eta(\tfrac{a}{1_R}) = f(a)f(1_R)^{-1} = f(a) \cdot 1_K = f(a)$$

για κάθε $a \in R$, οπότε $f = \eta \circ j$. Τέλος, εάν υποτεθεί ότι υφίσταται κάποιος μονομορφισμός $\eta' : \mathbf{Fr}(R) \longrightarrow K$ για τον οποίο ισχύει η ισότητα $f = \eta' \circ j$, τότε για κάθε $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \eta'(\tfrac{a}{b}) &= \eta'(j(a)j(b^{-1})) = \eta'(j(ab^{-1})) = (\eta' \circ j)(ab^{-1}) \\ &= f(ab^{-1}) = f(a)f(b)^{-1} = \eta(\tfrac{a}{b}), \end{aligned}$$

απ' όπου έπεται ότι $\eta' = \eta$. □

3.5.9 Πόρισμα. *Εάν η R είναι μια ακεραία περιοχή περιεχόμενη σε ένα σώμα K, τότε το*

$$\overline{R} := \left\{ ab^{-1} \,\middle|\, (a,b) \in R \times (R \smallsetminus \{0_R\}) \right\} \subseteq K$$

είναι το ελάχιστο υπόσωμα τού K (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την R και $\overline{R} \cong \mathbf{Fr}(R)$.

ΑΠΟΔΕΙΞΗ. Έστω $\iota : R \hookrightarrow K$ η συνήθης ένθεση. Επειδή η ι είναι μονομορφισμός, η πρόταση 3.5.8 μας πληροφορεί ότι υφίσταται ένας και μόνον μονομορφισμός σωμάτων $\eta : \mathbf{Fr}(R) \longrightarrow K$ με $\iota = \eta \circ j$, όπου j ο μονομορφισμός (3.25). Για κάθε $(a,b) \in R \times (R \smallsetminus \{0_R\})$ έχουμε

$$\eta(\tfrac{a}{b}) = \eta(j(a)j(b^{-1})) = \eta(j(ab^{-1})) = (\eta \circ j)(ab^{-1}) = \iota(ab^{-1}) = ab^{-1},$$

οπότε $\overline{R} = \mathrm{Im}(\eta) \cong \mathbf{Fr}(R)$. Επομένως, το $\overline{R}$ είναι αφ' εαυτού σώμα (βλ. 3.1.10 (iii)) με $R \subseteq \overline{R}$. Έστω τώρα τυχόν υπόσωμα L τού K περιέχον την ακεραία περιοχή R. Το L περιέχει το b^{-1} για κάθε $b \in R \smallsetminus \{0_R\}$. Κατά συνέπειαν, το L περιέχει όλα τα στοιχεία τής μορφής ab^{-1}, όπου $(a,b) \in R \times (R \smallsetminus \{0_R\})$. Αυτό σημαίνει ότι $R \subseteq L \subseteq \overline{R} \cong \mathbf{Fr}(R)$. □

3.5.10 Παράδειγμα. Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ περιέχεται (εξ ορισμού) στο σώμα $\mathbb{Q}(\sqrt{2})$ (βλ. άσκηση **1-37**). Επομένως,

$$\mathbb{Z}[\sqrt{2}] \subseteq \overline{\mathbb{Z}[\sqrt{2}]} = \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \subseteq \mathbb{Q}(\sqrt{2}).$$

Από την άλλη μεριά, κάθε στοιχείο τού $\mathbb{Q}(\sqrt{2})$ είναι τής μορφής $r + s\sqrt{2}$, όπου $r, s \in \mathbb{Q}$. Γράφοντας τα r, s ως κλάσματα $r = \frac{a}{b}$, $s = \frac{c}{d}$, για κατάλληλα ζεύγη $(a,b),(c,d) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, παρατηρούμε ότι

$$r + s\sqrt{2} = \tfrac{a}{b} + \tfrac{c}{d}\sqrt{2} = \tfrac{ad + cb\sqrt{2}}{bd} \in \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbf{Fr}(\mathbb{Z}[\sqrt{2}]).$$

Εκ των ανωτέρω έπεται ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$.

3.5.11 Πόρισμα. *Για κάθε σώμα K υφίσταται ισομορφισμός $K \cong \mathbf{Fr}(K)$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού πορίσματος 3.5.9 στην ειδική περίπτωση κατά την οποία $R = K$ (καθόσον $\overline{K} = K$). □

3.5.12 Πρόταση. *Έστω $f : R_1 \longrightarrow R_2$ ένας ομομορφισμός ακεραίων περιοχών. Τότε η απεικόνιση*

$$\mathbf{Fr}(f) : \mathbf{Fr}(R_1) \longrightarrow \mathbf{Fr}(R_2),\ \mathbf{Fr}(f)(\tfrac{a}{b}) := \tfrac{f(a)}{f(b)},\ \forall\, (a,b) \in R_1 \times (R_1 \smallsetminus \{0_{R_1}\}),$$

η επαγομένη μέσω τού f είναι ομομορφισμός σωμάτων. Επιπροσθέτως, ισχύουν τα εξής:

(i) *Εάν ο f είναι μονομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι μονομορφισμός.*

(ii) *Εάν ο f είναι επιμορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι επιμορφισμός.*

(iii) *Εάν ο f είναι ισομορφισμός, τότε και ο $\mathbf{Fr}(f)$ είναι ισομορφισμός, οπότε*

$$R_1 \cong R_2 \Longrightarrow \mathbf{Fr}(R_1) \cong \mathbf{Fr}(R_2).$$

ΑΠΟΔΕΙΞΗ. Η $\mathbf{Fr}(f)$ είναι *ομομορφισμός* σωμάτων, διότι για $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ έχουμε

$$\begin{aligned} \mathbf{Fr}(f)(\tfrac{a}{b} + \tfrac{c}{d}) &= \mathbf{Fr}(f)(\tfrac{ad+cb}{bd}) = \tfrac{f(ad+cb)}{f(bd)} = \tfrac{f(ad)+f(cb)}{f(b)f(d)} = \tfrac{f(a)f(d)+f(c)f(b)}{f(b)f(d)} \\ &= \tfrac{f(a)}{f(b)} + \tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b}) + \mathbf{Fr}(f)(\tfrac{c}{d}) \end{aligned}$$

και

$$\begin{aligned} \mathbf{Fr}(f)(\tfrac{a}{b} \cdot \tfrac{c}{d}) &= \mathbf{Fr}(f)(\tfrac{ac}{bd}) = \tfrac{f(ac)}{f(bd)} = \tfrac{f(a)f(c)}{f(b)f(d)} \\ &= \tfrac{f(a)}{f(b)} \tfrac{f(c)}{f(d)} = \mathbf{Fr}(f)(\tfrac{a}{b})\mathbf{Fr}(f)(\tfrac{c}{d}). \end{aligned}$$

(i) Εάν η f είναι ενριπτική, τότε και η απεικόνιση $\mathbf{Fr}(f)$ είναι ενριπτική, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R_1)$ με $\mathbf{Fr}(f)(\frac{a}{b}) = \mathbf{Fr}(\frac{c}{d})$, τότε $\frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$, απ' όπου έπεται ότι

$$f(a)f(d) = f(c)f(b) \Longrightarrow f(ad) = f(cb) \underset{[f \text{ ενριπτική}]}{\Longrightarrow} ad = cb \Longrightarrow \tfrac{a}{b} = \tfrac{c}{d}.$$

(ii) Εάν η f είναι επιρριπτική, τότε και η $\mathbf{Fr}(f)$ είναι επιρριπτική, διότι για κάθε $\frac{c}{d} \in \mathbf{Fr}(R_2)$ υπάρχει ζεύγος $(a,b) \in R_1 \times (R_1 \smallsetminus \{0_{R_1}\})$, τέτοιο ώστε να ισχύει

$$[f(a) = c, \quad f(b) = d] \Longrightarrow \mathbf{Fr}(f)(\tfrac{a}{b}) = \tfrac{f(a)}{f(b)},$$

ήτοι $\mathbf{Fr}(f)(\frac{a}{b}) = \frac{c}{d}$. Το (iii) είναι άμεση συνέπεια των (i) και (ii). □

3.6 ΠΡΩΤΑ ΣΩΜΑΤΑ

Έστω L ένα υπόσωμα τού σώματος $\mathbb{Q}$ των ρητών αριθμών. Επειδή υπάρχει πάντοτε κάποιο $a \in L \smallsetminus \{0\}$, η -εξ ορισμού εγγυηθείσα- ύπαρξη τού (πολλαπλασιαστικού) αντιστρόφου του a^{-1} έχει ως επακόλουθο το ότι

$$a^{-1}a = 1_L = 1_{\mathbb{Q}} \in L.$$

Ως εκ τούτου, για κάθε ακέραιο $n \in \mathbb{Z}$ ισχύει $n = n \cdot 1_L = n \cdot 1_{\mathbb{Q}} \in L$, οπότε έχουμε κατ' ανάγκην την εγκλειστική σχέση $\mathbb{Z} \subseteq L \subseteq \mathbb{Q}$. Όμως, σύμφωνα με το πόρισμα 3.5.9, το $\mathbb{Q} = \mathbf{Fr}(\mathbb{Z})$ είναι το ελάχιστο σώμα (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την ακεραία περιοχή $\mathbb{Z}$. Άρα τελικώς $L = \mathbb{Q}$. Η ιδιότητα αυτή τού $\mathbb{Q}$ το καθιστά το πλέον τυπικό παράδειγμα των λεγομένων «πρώτων σωμάτων».

3.6.1 Ορισμός. Ένα σώμα K καλείται **πρώτο σώμα** όταν δεν περιέχει κανένα γνήσιο υπόσωμα.

3.6.2 Παράδειγμα. Πέραν τού $\mathbb{Q}$, ένα άλλο πρώτο σώμα είναι το $\mathbb{Z}_p$, όπου p πρώτος αριθμός. Πράγματι· εάν το L είναι ένα υπόσωμα τού $\mathbb{Z}_p$, τότε η (προσθετική) υποομάδα $(L, +)$ τής ομάδας $(\mathbb{Z}_p, +)$ είναι πεπερασμένη με τάξη της έναν διαιρέτη τού p (λόγω τού θεωρήματος τού Lagrange). Επειδή λοιπόν ο p είναι πρώτος, $|L| = 1$ ή $|L| = p$. Η πρώτη περίπτωση αποκλείεται, καθότι το L -ως σώμα- έχει τάξη $|L| \geq 2$. Επομένως, $|L| = p$, οπότε κατ' ανάγκην $L = \mathbb{Z}_p$.

3.6.3 Θεώρημα. *Κάθε σώμα K περιέχει ένα και μόνον πρώτο υπόσωμα.*

ΑΠΟΔΕΙΞΗ. Το σώμα

$$K_0 := \bigcap \{ S \mid S \text{ υπόσωμα τού } K \} \subseteq K$$

είναι ένα πρώτο υπόσωμα τού K. Πράγματι· εάν το L είναι ένα υπόσωμα τού K_0, τότε το L είναι και υπόσωμα τού K, οπότε $K_0 \subseteq L$, απ' όπου συμπεραίνουμε ότι $L = K_0$. Υπολείπεται η απόδειξη τής μοναδικότητας τού K_0. Υποτιθεμένης τής υπάρξεως ενός άλλου πρώτου υποσώματος K_0' τού σώματος K, το $K_0 \cap K_0'$ είναι υπόσωμα τού K και $K_0 \cap K_0' \subseteq K_0$, $K_0 \cap K_0' \subseteq K_0'$. Επομένως, $K_0 \cap K_0' = K_0$ και $K_0 \cap K_0' = K_0'$, πράγμα που σημαίνει ότι $K_0 = K_0'$. □

3.6.4 Θεώρημα. (i) *Κάθε πρώτο σώμα χαρακτηριστικής μηδέν είναι ισόμορφο με το σώμα $\mathbb{Q}$ των ρητών αριθμών.*

(ii) *Κάθε πρώτο σώμα χαρακτηριστικής p (όπου p πρώτος αριθμός) είναι ισόμορφο με το σώμα $\mathbb{Z}_p$ των κλάσεων ισοτιμιών κατά μόδιο p.*

ΑΠΟΔΕΙΞΗ. Έστω L ένα πρώτο σώμα. Ορίζουμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow L, \quad f(n) := n \cdot 1_L, \ \ \forall n \in \mathbb{Z}.$$

Επειδή

$$\begin{cases} f(m+n) = (m+n) \cdot 1_L = m \cdot 1_L + n \cdot 1_L = f(m) + f(n), \\ f(mn) = (mn) \cdot 1_L = m\,(n \cdot 1_L) = (m \cdot 1_L)\,(n \cdot 1_L) = f(m)f(n), \end{cases}$$

για οιουσδήποτε $m, n \in \mathbb{Z}$, η f είναι ένας ομομορφισμός δακτυλίων. Βάσει τού 1ου θεωρήματος ισομορφισμών 3.3.3,

$$\mathbb{Z}/\mathrm{Ker}\,(f) \cong \mathrm{Im}\,(f) = f(\mathbb{Z}),$$

όπου

$$\mathrm{Ker}\,(f) = \{\, n \in \mathbb{Z} \mid n \cdot 1_L = 0_L \}.$$

(i) Εάν το L έχει χαρακτηριστική μηδέν, τότε $\mathrm{Ker}(f) = \{0\}$, οπότε

$$\mathbb{Z}/\mathrm{Ker}\,(f) = \mathbb{Z}/\{0\} \cong \mathbb{Z} \cong \mathrm{Im}\,(f) = f(\mathbb{Z}).$$

Ως εκ τούτου, η $\mathrm{Im}\,(f)$ είναι μια ακεραία περιοχή (ισόμορφη με τον $\mathbb{Z}$) και, επειδή $\mathrm{Im}\,(f) \subseteq L$, έχουμε

$$\mathbf{Fr}\,(\mathrm{Im}\,(f)) = \left\{ \frac{n \cdot 1_L}{m \cdot 1_L} \;\middle|\; (n,m) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \right\} \subseteq \mathbf{Fr}\,(L) \cong L,$$

οπότε $L \cong \mathbf{Fr}\,(L) = \mathbf{Fr}\,(\mathrm{Im}\,(f)) \cong \mathbf{Fr}\,(\mathbb{Z}) = \mathbb{Q}$ (λόγω τής προτάσεως 3.5.12 και τού ότι το L είναι πρώτο σώμα).

(ii) Εάν το L έχει χαρακτηριστική p, όπου p πρώτος αριθμός, τότε, βάσει τής προτάσεως 1.4.3 έχουμε

$$p = \min \{\, |k| \in \mathbb{N} \mid k \in \mathbb{Z} \smallsetminus \{0\} \ \text{ με } \ k \cdot 1_L = 0_L \},$$

οπότε $p \in \mathrm{Ker}(f) \Longrightarrow p\mathbb{Z} = \langle p \rangle \subseteq \mathrm{Ker}(f)$. Αλλά και για κάθε $\lambda \in \mathrm{Ker}(f)$, γράφοντας

$$\lambda = up + r, \ \ u, r \in \mathbb{Z}, \quad 0 \leq r \leq p - 1,$$

λαμβάνουμε

$$0_L = \lambda \cdot 1_L = u\,(p \cdot 1_L) + (r \cdot 1_L) = 0_L + r \cdot 1_L = r \cdot 1_L,$$

ήτοι μια ισότητα η οποία (λόγω τής ως άνω συνθήκης ελαχίστου που πληροί το p) ισχύει μόνον όταν $r = 0$. Επομένως, $\lambda \in \langle p \rangle$, οπότε $\mathrm{Ker}(f) \subseteq p\mathbb{Z} = \langle p \rangle$. Τελικώς λοιπόν $\mathrm{Ker}(f) = p\mathbb{Z} = \langle p \rangle$ και

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p \cong \mathrm{Im}\,(f) = f(\mathbb{Z}) = \{\, n \cdot 1_L \mid n \in \{0, 1, \ldots, p-1\}\} \subseteq L,$$

απ' όπου συμπεραίνουμε ότι $L = \mathrm{Im}\,(f) \cong \mathbb{Z}_p$, διότι το L είναι πρώτο σώμα. $\square$

3.6.5 Πόρισμα. *Κάθε σώμα K περιέχει ένα υπόσωμα L, τέτοιο ώστε:*

$$L \cong \begin{cases} \mathbb{Q}, & \text{όταν } \chi\alpha\varrho(K) = 0, \\ \mathbb{Z}_p, & \text{όταν } \chi\alpha\varrho(K) = p > 0. \end{cases}$$

3.6.6 Παρατήρηση. Σύμφωνα με όσα αναφέραμε στην απόδειξη τού θεωρήματος 3.6.4, εάν το L είναι ένα πρώτο σώμα, τότε

$$L \cong \left\{ (n \cdot 1_L)\,(m \cdot 1_L)^{-1} \;\middle|\; (n,m) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}) \right\}, \quad \text{όταν } \chi\alpha\varrho(L) = 0,$$

και

$$L = \;\{ n \cdot 1_L \mid n \in \{0, 1, \ldots, p-1\}\}, \quad \text{όταν } \chi\alpha\varrho(L) = p > 0.$$

Ασκήσεις

3-1. Ποιες εκ των ακολούθων απεικονίσεων $f : R \longrightarrow R'$ είναι ομομορφισμοί δακτυλίων;

(i) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k]_m \,.$$

(ii) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k+1]_m \,.$$

(iii) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a.$$

(iv) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a + d.$$

(v) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := ad - bc.$$

(vi) $R = \mathbb{Z}$, $R' = \mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := \begin{pmatrix} [1]_m & [0]_m \\ [0]_m & [k]_m \end{pmatrix}.$$

3-2. (i) Να αποδειχθεί ότι η απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5,\ n \longmapsto f(n) := ([n]_3\,, [n]_5),$$

είναι επιμορφισμός και να προσδιορισθεί ο πυρήνας $\mathrm{Ker}(f)$.

(ii) Να προσδιορισθούν όλοι οι ομομορφισμοί $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_{12}$.

3-3. Να αποδειχθεί ότι οι μόνοι ενδομορφισμοί τού $\mathbb{Z}$ είναι ο μηδενικός ομομορφισμός και ο ταυτοτικός $\mathrm{id}_{\mathbb{Z}}$.

3-4. Έστω $m \in \mathbb{N}$. Να αποδειχθεί ότι κάθε ενδομορφισμός $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ τού $\mathbb{Z}_m$ ορίζεται μέσω ενός τύπου τής μορφής

$$f([k]_m) = [a]_m\,[k]_m\,,\ \forall k \in \mathbb{Z},$$

για κάποιον ακέραιο a, τέτοιον ώστε το στοιχείο $[a]_m \in \mathbb{Z}_m$ να είναι ταυτοδύναμο.

3-5. Να αποδειχθεί ότι για κάθε ακέραιο m στερούμενον τετραγώνων η απεικόνιση

$$\mathbb{Q}(\sqrt{m}) \ni a + b\sqrt{m} \longmapsto a - b\sqrt{m} \in \mathbb{Q}(\sqrt{m}),\ \ a, b \in \mathbb{Z},$$

είναι αυτομορφισμός τού σώματος $\mathbb{Q}(\sqrt{m})$ (βλ. το (iv) τής ασκήσεως **1-37**).

3-6. Έστω K ένα σώμα με $\chi\alpha\rho(K) = p > 0$ και έστω

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

η απεικόνιση τού Frobenius (βλ. 3.1.2 (iv)) Να αποδειχθούν τα εξής:

(i) Η f είναι μονομορφισμός. [*Υπόδειξη*: Βλ. πρόταση 3.1.11.]

(ii) Όταν το K είναι πεπερασμένο σώμα, τότε η f είναι ισομορφισμός (ήτοι αυτομορφισμός τού K).

(iii) Όταν το K είναι απειροπληθές, τότε η f είναι δεν είναι κατ' ανάγκην ισομορφισμός. [*Υπόδειξη*: Να εξετασθεί τι συμβαίνει στην περίπτωση κατά την οποία το K είναι το σώμα $\mathbb{Z}_p(\mathsf{X})$ των ρητών συναρτήσεων υπεράνω τού σώματος $\mathbb{Z}_p$.]

3-7. Έστω R ένας δακτύλιος και έστω $f : R \longrightarrow R$ ένας ενδομορφισμός αυτού. Να αποδειχθεί ότι το $S := \{ r \in R |\ f(r) = r \}$ είναι ένας υποδακτύλιος τού R.

3-8. Έστω R ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Εάν $a \in R^{\times}$, να αποδειχθεί ότι η απεικόνιση

$$f_a : R \longrightarrow R,\ \ r \longmapsto f_a(r) := ara^{-1},$$

είναι ένας αυτομορφισμός τού R.

3-9. Εάν οι $f : R \longrightarrow R'$ και $g : R' \longrightarrow R''$ είναι δυο ομομορφισμοί δακτυλίων, να αποδειχθεί ότι ισχύουν οι εγκλεισμοί:

$$\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g \circ f), \ \ \mathrm{Im}(g \circ f) \subseteq \mathrm{Im}(g).$$

και ότι εξ αυτών έπονται άμεσα οι συνεπαγωγές

$$g \circ f \text{ μονομορφισμός } \Rightarrow f \text{ μονομορφισμός}$$

και

$$g \circ f \ \text{ επιμορφισμός } \Rightarrow g \text{ επιμορφισμός.}$$

Εν συνεχεία, να παρατεθούν παραδείγματα ομομορφισμών

$$f : R \longrightarrow R' \ \text{ και } \ g : R' \longrightarrow R'',$$

ούτως ώστε

(i) η σύνθεση $g \circ f$ να είναι και ο g να μην είναι μονομορφισμός,

(ii) η σύνθεση $g \circ f$ να είναι και ο f να μην είναι επιμορφισμός, και

(iii) η $g \circ f$ να είναι ισομορφισμός και κανείς εκ των f, g να μην είναι ισομορφισμός.

3-10. Έστω $f : R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων. Να αποδειχθούν τα εξής:

(i) $f(Z(R)) \subseteq Z(R')$ (βλ. άσκηση **1-14**).

(ii) Εάν το $a \in R$ είναι ταυτοδύναμο στοιχείο, τότε και το $f(a) \in R'$ είναι ταυτοδύναμο.

(iii) Εάν το $a \in R$ είναι μηδενοδύναμο στοιχείο, τότε και το $f(a) \in R'$ είναι μηδενοδύναμο (οπότε $f(\mathrm{Nil}(R)) \subseteq \mathrm{Nil}(R')$).

Εν συνεχεία, να δοθούν παραδείγματα επιμορφισμών δακτυλίων για τους οποίους ο εγκλεισμός στο (i) είναι αυστηρός και τα αντίστροφα των (ii) και (iii) αναληθή.

3-11. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού R, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f\,(I + J) = f\,(I) + f\,(J)\,,$

(ii) $f\,(I\,J) = f\,(I)\ f\,(J)\,,$

(iii) $f\,(I \cap J) \subseteq f\,(I)\ \cap f\,(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\mathrm{Ker}(f) \subseteq I$ ή $\mathrm{Ker}(f) \subseteq J$).

(iv) Εάν ο R (και -κατ' επέκτασιν- και ο S, λόγω τής 3.1.4 (vii)) είναι μεταθετικός, τότε $f\,(I : J) \subseteq f\,(I)\ : f\,(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\mathrm{Ker}(f) \subseteq I$).

(v) Εάν ο R είναι μεταθετικός, τότε $f(\mathrm{Rad}(I)) \subseteq \mathrm{Rad}(f(I))$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\mathrm{Ker}(f) \subseteq I$).

3-12. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού S, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f^{-1}(I + J) = f^{-1}(I) + f^{-1}(J)$,

(ii) $f^{-1}(I\,J) \supseteq f^{-1}(I)\, f^{-1}(J)$, (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\mathrm{Ker}(f) \subseteq f^{-1}(I)\, f^{-1}(J)$),

(iii) $f^{-1}(I \cap J) = f^{-1}(I) \cap f^{-1}(J)$.

(iv) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(I : J) = f^{-1}(I) : f^{-1}(J)$.

(v) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(\mathrm{Rad}(I)) = \mathrm{Rad}\big(f^{-1}(I)\big)$.

3-13. Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Υποτιθεμένου ότι $\chi\alpha\varrho(R) > 0$, να αποδειχθεί ότι $\chi\alpha\varrho(f(R)) \leq \chi\alpha\varrho(R)$.

3-14. Να αποδειχθεί ότι ισόμορφοι δακτύλιοι έχουν ίσες χαρακτηριστικές.

3-15. Εάν R και R' είναι δυο δακτύλιοι με μοναδιαίο στοιχείο, να αποδειχθεί ότι δεν υφίστανται ομομορφισμοί $f : R \longrightarrow R'$ με $f(1_R) = 1_{R'}$ όταν ικανοποιείται μία εκ των κάτωθι συνθηκών:

(i) $\chi\alpha\varrho(R) > 0 = \chi\alpha\varrho(R')$.

(ii) $\chi\alpha\varrho(R) > 0$, $\chi\alpha\varrho(R') > 0$ και $\chi\alpha\varrho(R') \nmid \chi\alpha\varrho(R)$.

3-16. Εάν $f : K \longrightarrow L$ είναι ένας ομορφισμός στρεβλών σωμάτων με $f(1_R) = 1_{R'}$, να αποδειχθεί ότι $\chi\alpha\varrho(K) = \chi\alpha\varrho(L)$.

3-17. Έστω $f : R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων. Να αποδειχθούν τα εξής:

(i) Ο R' είναι ακεραία περιοχή εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι πρώτο ιδεώδες τού R.

(ii) Ο R' είναι σώμα εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι μεγιστικό ιδεώδες τού R.

3-18. Να αποδειχθεί ότι δεν υφίστανται ομομορφισμοί $f : \mathbb{C} \longrightarrow S$ (από το σώμα των μιγαδικών αριθμών σε έναν δακτύλιο S) με $\mathrm{Ker}(f) = \mathbb{Z}$.

3-19. Να αποδειχθεί ότι $\mathbb{Z}[\sqrt{3}] \ncong \mathbb{Z}[\sqrt{5}]$ και $\mathbb{Z}[\mathsf{X}] \ncong \mathbb{Q}[\mathsf{X}]$.

3-20. Έστω $f : R \longrightarrow S$ ένας ισομορφισμός δακτυλίων με μοναδιαία στοιχεία. Να αποδειχθούν τα ακόλουθα:

(i) Έστω $r \in R$. Τότε $r \in R^{\times} \Leftrightarrow f(r) \in S^{\times}$.

(ii) Η απεικόνιση $R^{\times} \ni r \longmapsto f(r) \in S^{\times}$ είναι αμφιρριπτική.

3-21. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν υποτεθεί ότι κάθε υποδακτύλιος τού R είναι ιδεώδες, να αποδειχθεί ότι ο R είναι *είτε* τετριμμένος *είτε* ισόμορφος με τον δακτύλιο $\mathbb{Z}$ των ακεραίων *είτε* ισόμορφος με τον δακτύλιο $\mathbb{Z}_m$, όπου $m \in \mathbb{N}$, $m \geq 2$. [*Υπόδειξη*: Να χρησιμοποιηθεί ο ομομορφισμός δακτυλίων $f : \mathbb{Z} \longrightarrow R$, $n \longmapsto f(n) := n \cdot 1_R$, το 1ο θεώρημα ισομορφισμών 3.3.3 και η πρόταση 2.2.6.]

3-22. Έστω M ένα μη κενό σύνολο και έστω $(\mathfrak{P}(M), \triangle, \cap)$ ο δακτύλιος ο ορισθείς στην άσκηση **1-7**. Να αποδειχθούν τα ακόλουθα για οιοδήποτε $E \subseteq M$:

(i) Το $\mathfrak{P}(E)$ είναι ένα ιδεώδες τού $\mathfrak{P}(M)$.

(ii) Η απεικόνιση

$$f_E : \mathfrak{P}(M) \longrightarrow \mathfrak{P}(M), \;\; A \longmapsto f_E(A) := A \cap (M \smallsetminus E)$$

είναι ομομορφισμός.

(iii) $\mathfrak{P}(M) / \mathfrak{P}(E) \cong \mathfrak{P}(M \smallsetminus E)$.

3-23. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο

$$S := \left\{ \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

αποτελεί έναν υποδακτύλιο τού $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

(ii) Η απεικόνιση $f : \mathbb{Z}[\sqrt{m}] \longrightarrow S$ η οριζόμενη από τον τύπο

$$\mathbb{Z}[\sqrt{m}] \ni a + b\sqrt{m} \overset{f}{\longmapsto} \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \in S$$

είναι ένας ισομορφισμός δακτυλίων. Ως εκ τούτου, ο S είναι μια ακεραία περιοχή. (Βλ. άσκηση **1-37** και το (i) τού πορίσματος 3.1.10.)

3-24. Να αποδειχθεί ότι $\mathbb{R}[\mathsf{X}] / \left\langle \mathsf{X}^2 \right\rangle \cong S$, όπου

$$S := \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \;\middle|\; a, b \in \mathbb{R} \right\}.$$

[*Υπόδειξη*: Να δειχθεί ότι η απεικόνιση

$$\mathbb{R}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto \left(\begin{array}{cc} a_0 & a_1 \\ 0 & a_0 \end{array} \right) \in S$$

είναι επιμορφισμός δακτυλίων έχων το κύριο ιδεώδες $\left\langle \mathsf{X}^2 \right\rangle$ ως πυρήνα του και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-25. Εάν $I := \left\langle \mathsf{X}^2 + 1 \right\rangle$ και $J := \left\langle \mathsf{X}^2 + 2 \right\rangle \subsetneqq \mathbb{R}[\mathsf{X}]$, να αποδειχθεί ότι

$$\mathbb{R}[\mathsf{X}]/I \cong \mathbb{R}[\mathsf{X}]/J \;\text{ και }\; I \neq J.$$

3-26. Να αποδειχθούν τα ακόλουθα:

(i) Το ιδεώδες $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$ είναι πρώτο ιδεώδες τού $\mathbb{Z}[\mathsf{X}_1, \mathsf{X}_2]$ αλλά δεν είναι μεγιστικό.

(ii) Το ιδεώδες $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$ είναι μεγιστικό ιδεώδες τού $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$.

[*Υπόδειξη*: Εάν $R \in \{\mathbb{Z}, \mathbb{Q}\}$, να δειχθεί ότι η απεικόνιση

$$R[\mathsf{X}_1, \mathsf{X}_2] \ni \sum a_{ij} \mathsf{X}_1^i \mathsf{X}_2^j \longmapsto a_{00} \in R$$

είναι επιμορφισμός δακτυλίων έχων ως πυρήνα του το $\langle \mathsf{X}_1, \mathsf{X}_2 \rangle$. Κατόπιν τούτου, να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3 σε συνδυασμό με το θεώρημα 2.6.4 και το πόρισμα 2.6.5.]

(iii) Έστω τυχόν $\xi \in [0,1]$. Τότε το $\mathfrak{m}_\xi := \{\, f \in \mathcal{C}([0,1]) \mid f(\xi) = 0\}$ είναι ένα μεγιστικό ιδεώδες τού δακτυλίου

$$\mathcal{C}([0,1]) := \left\{ f \in \mathbb{R}^{[0,1]} \;\middle|\; f \;\text{ συνεχής} \right\}$$

(βλ. άσκηση **1-30**). [*Υπόδειξη*: Να χρησιμοποιηθεί ο ομομορφισμός

$$\psi_\xi : \mathcal{C}([0,1]) \longrightarrow \mathbb{R}$$

ο οριζόμενος από τον τύπο $\psi_\xi(f) := f(\xi)$, καθώς και το 1ο θεώρημα ισομορφισμών 3.3.3.]

(iv) Ένα ιδεώδες I τού $\mathcal{C}([0,1])$ είναι μεγιστικό εάν και μόνον εάν $\exists \xi \in [0,1]$: $I = \mathfrak{m}_\xi$. [*Υπόδειξη*: Να γίνει κατάλληλη χρήση τής συμπάγειας τού κλειστού διαστήματος $[0,1]$.]

3-27. Έστω m ένας *θετικός* ακέραιος στερούμενος τετραγώνων και έστω

$$I_p(\sqrt{m}) := \left\{ a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \;\middle|\; \text{με } \; p \mid a \text{ και } \; p \mid b \right\} \subsetneqq \mathbb{R},$$

όπου p περιττός πρώτος με $p \nmid m$. Να αποδειχθούν τα εξής:

(i) Το $I_p(\sqrt{m})$ είναι ένα ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$.

(ii) Εάν $n^2 \not\equiv m (\operatorname{mod} p)$, $\forall n \in \mathbb{Z}$, τότε το $I_p(\sqrt{m})$ είναι ένα μεγιστικό ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$ και ο πηλικοδακτύλιος $\mathbb{Z}[\sqrt{m}]/I_p(\sqrt{m})$ ένα σώμα με p^2 στοιχεία.

3-28. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R (όπου $n \in \mathbb{N}$, $n \geq 2$), τότε το άθροισμά τους $I = I_1 + \cdots + I_n$ καλείται **(εσωτερικό) ευθύ άθροισμα**, σημειούμενο μέσω τού ειδικού συμβόλου $I_1 \oplus \cdots \oplus I_n$, όταν κάθε στοιχείο $a \in I$ εκφράζεται *μονοσημάντως* ως

$$a = a_1 + \cdots + a_n, \ \ a_j \in I_j, \ \ \forall j \in \{1, \ldots, n\}.$$

Να αποδειχθεί η ισοδυναμία των ακολούθων συνθηκών:

(i) Το I είναι το ευθύ άθροισμα των $I_1, \ldots, I_n$.

(ii) Εάν $0_R = a_1 + \cdots + a_n$, όπου $a_j \in I_j, \ \forall j \in \{1, \ldots, n\}$, τότε

$$a_1 = \cdots = a_n = 0_R.$$

(iii) $I_j \cap (\sum\limits_{k \in \{1,\ldots,n\} \smallsetminus \{j\}} I_k) = \{0_R\}, \ \ \forall j \in \{1, \ldots, n\}.$

3-29. Να αποδειχθούν τα ακόλουθα:

(i) Εάν $R = R_1 \times \cdots \times R_n$ είναι το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ (όπου $n \in \mathbb{N}, \ n \geq 2$), και

$$\widetilde{R}_j := \left\{ \left(0_{R_1}, \ldots, 0_{R_{j-1}}, a_j, 0_{R_{j+1}} \ldots, 0_{R_n}\right) \in R \;\middle|\; a_j \in R_j \right\},$$

τότε $R = \widetilde{R}_1 \oplus \cdots \oplus \widetilde{R}_n$, όπου τα $\widetilde{R}_j$ και R_j είναι ισόμορφοι ως δακτύλιοι.

(ii) Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R (όπου $n \in \mathbb{N}, \ n \geq 2$), και $R = I_1 \oplus \cdots \oplus I_n$, τότε

$$\boxed{R \cong I_1 \times \cdots \times I_n,}$$

με καθένα των $I_1, \ldots, I_n$ θεωρούμενο ως «αυτόνομος» δακτύλιος (ήτοι ως το «εξωτερικό» ευθύ γινόμενο των $I_1, \ldots, I_n$).

3-30. Έστω $R = R_1 \times \cdots \times R_n$ το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ με μοναδιαία στοιχεία (όπου $n \in \mathbb{N}, \ n \geq 2$). Να αποδειχθούν τα εξής:

(i) Για κάθε $j \in \{1, \ldots, n\}$ η **φυσική προβολή** pr_j **τού** R **επί τού** R_j η οριζόμενη από τον τύπο

$$\mathrm{pr}_j : R \longrightarrow R_j, \ (a_1, \ldots, a_n) \longmapsto \mathrm{pr}_j(a_1, \ldots, a_n) := a_j,$$

είναι επιμορφισμός δακτυλίων.

(ii) Κάθε ιδεώδες I τού R είναι τής μορφής

$$\boxed{I = I_1 \oplus \cdots \oplus I_n \cong I_1 \times \cdots \times I_n,}$$

όπου I_j κάποιο ιδεώδες τού R_j, για κάθε $j \in \{1, \ldots, n\}$. [*Υπόδειξη*: Αρκεί να τεθεί $I_j := \mathrm{pr}_j(I)$.]

(iii) Ένα γνήσιο ιδεώδες I τού R είναι μεγιστικό εάν και μόνον εάν αυτό είναι τής μορφής

$$\begin{aligned} I &= R_1 \oplus \cdots \oplus R_{j-1} \times \mathfrak{m}_j \oplus R_{j+1} \oplus \cdots \oplus R_n \\ &\cong R_1 \times \cdots \times R_{j-1} \times \mathfrak{m}_j \times R_{j+1} \times \cdots \times R_n, \end{aligned}$$

όπου το $\mathfrak{m}_j$ είναι ένα μεγιστικό ιδεώδες τού R_j για κάποιον $j \in \{1, \ldots, n\}$.

3-31. Εάν τα I_1, I_2 είναι δυο ιδεώδη ενός δακτυλίου R και $R = I_1 \oplus I_2$, να αποδειχθεί ότι

$$R/I_1 \cong I_2 \text{ και } R/I_2 \cong I_1.$$

3-32. Έστω $R = R_1 \times \cdots \times R_n$ το ευθύ γινόμενο n δακτυλίων $R_1, \ldots, R_n$ (όπου $n \in \mathbb{N}$, $n \geq 2$). Εάν το I_j είναι ένα ιδεώδες τού R_j για κάθε $j \in \{1, \ldots, n\}$ και $I := I_1 \oplus \cdots \oplus I_n$,να αποδειχθεί ότι

$$\boxed{R/I \cong (R_1/I_1) \oplus \cdots \oplus (R_n/I_n).}$$

[*Υπόδειξη*: Για κάθε $j \in \{1, \ldots, n\}$ να δειχθεί ότι η απεικόνιση

$$f : R \longrightarrow (R_1/I_1) \times \cdots \times (R_n/I_n) \cong (R_1/I_1) \oplus \cdots \oplus (R_n/I_n)$$
$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n) := (\pi_{I_1}^{R_1}(a_1), \ldots, \pi_{I_n}^{R_n}(a_n))$$

είναι επιμορφισμός δακτυλίων με πυρήνα $\mathrm{Ker}(f) = I$ και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-33. (i) Εάν οι R και S είναι δυο δακτύλιοι και $I = \{(r, 0_S) \mid r \in R\}$, να αποδειχθεί ότι το I είναι ιδεώδες τού $R \times S$ και ότι

$$(R \times S)/I \cong S.$$

(ii) Εάν $m, n \in \mathbb{N}$, να αποδειχθεί ότι

$$(\mathbb{Z} \times \mathbb{Z})/(m\mathbb{Z} \times n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

3-34. Έστω R ένας μεταθετικός δακτύλιος ο οποίος περιέχει ένα ταυτοδύναμο στοιχείο c. Εάν

$$I := \{a \in R \mid ac = 0_R\}, \quad J := \{a \in R \mid ac = a\},$$

να αποδειχθούν τα ακόλουθα:

(i) Τα I και J είναι ιδεώδη τού R.

(ii) $J = \langle c \rangle$.

(iii) $R \cong I \times J$.

(iv) $IJ = \{0_R\}$.

3-35. Έστω ότι ο R είναι ένας δακτύλιος, ο S ένας υποδακτύλιος τού R και το I ένα ιδεώδες τού R. Εάν $S \cap I = \{0_R\}$, να αποδειχθεί ότι ο S είναι ισόμορφος με έναν υποδακτύλιο τού πηλικοδακτυλίου R/I. [*Υπόδειξη*: Να χρησιμοποιηθεί το 2ο θεώρημα ισομορφισμών 3.3.15.]

3-36. Να προσδιορισθούν όλα τα πρώτα και τα μεγιστικά ιδεώδη τού δακτυλίου $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ (για οιονδήποτε $m \in \mathbb{N}$), καθώς και η τομή όλων των μεγιστικών ιδεωδών αυτού.

3-37. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω τυχόν $f(\mathsf{X}) \in R[\mathsf{X}]$. Εάν

$$\varphi(\mathsf{X}) = \sum\nolimits_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],$$

τότε μέσω τής απεικονίσεως

$$\mathfrak{v}_{\varphi(\mathsf{X})} : R \longrightarrow R, \quad r \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}(r) := \varphi(r) := \sum_{i=1}^{n} a_i r^i.$$

τής επαγομένης από το $\varphi(\mathsf{X})$ ορίζεται η απεικόνιση

$$R\,[\mathsf{X}] \longrightarrow \text{ΑΠ}\,(R, R) = R^R, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}.$$

καθώς και η **απεικόνιση πολυωνυμικής αποτιμήσεως σε ένα** (παγιωμένο) **στοιχείο** $r \in R$:

$$\boldsymbol{\varepsilon}_r : R\,[\mathsf{X}] \longrightarrow R, \quad \varphi(\mathsf{X}) \longmapsto \boldsymbol{\varepsilon}_r(\,\varphi(\mathsf{X})) := \mathfrak{v}_{\varphi(\mathsf{X})}(r) := \varphi(r)$$

(βλ. 1.3.11). Να αποδειχθούν τα ακόλουθα:

(i) Η $R\,[\mathsf{X}] \ni \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})} \in R^R$ είναι ομομορφισμός δακτυλίων και είναι, ιδιαιτέρως, επιμορφισμός όταν $R = \mathbb{Z}_p$, όπου p πρώτος αριθμός, ενώ δεν είναι επιμορφισμός όταν $R = \mathbb{R}$. [*Σημείωση*: Όπως έχει ήδη επισημανθεί στο εδάφιο 1.3.11, η $R\,[\mathsf{X}] \ni \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})} \in R^R$ δεν είναι κατ' ανάγκην μονομορφισμός και, ως εκ τούτου, ο $R\,[\mathsf{X}]$ δεν είναι πάντοτε εμφυτεύσιμος στον R^R.]

(ii) Η $\boldsymbol{\varepsilon}_r$ είναι επιμορφισμός για κάθε $r \in R$.

3-38. Δοθέντος ενός ομομορφισμού $f : R \longrightarrow S$ μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, να αποδειχθεί ότι οι απεικονίσεις

$$\begin{aligned} &\theta_f^{(1)} : R[\mathsf{X}] \longrightarrow S[\mathsf{X}], && \theta_f^{(2)} : R[\![\mathsf{X}]\!] \longrightarrow S[\![\mathsf{X}]\!], \\ &\theta_f^{(3)} : R[\mathsf{X}^{\pm 1}] \longrightarrow S[\mathsf{X}^{\pm 1}], && \theta_f^{(4)} : \mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \longrightarrow \mathrm{Laur}_S[\![\mathsf{X}^{\pm 1}]\!], \end{aligned}$$

οι οριζόμενες μέσω των τύπων

$$R[\mathsf{X}] \ni \textstyle\sum_{i=0}^{n} a_i\mathsf{X}^i \overset{\theta_f^{(1)}}{\longmapsto} \sum_{i=0}^{n} f(a_i)\mathsf{X}^i \in S[\mathsf{X}],\ n \in \mathbb{N}_0,$$

$$R[\![\mathsf{X}]\!] \ni \textstyle\sum_{i=0}^{\infty} a_i\mathsf{X}^i \overset{\theta_f^{(2)}}{\longmapsto} \sum_{i=0}^{\infty} f(a_i)\mathsf{X}^i \in S[\![\mathsf{X}]\!],$$

$$R[\mathsf{X}^{\pm 1}] \ni \textstyle\sum_{i=-n}^{m} a_i\mathsf{X}^i \overset{\theta_f^{(3)}}{\longmapsto} \sum_{i=-n}^{m} f(a_i)\mathsf{X}^i \in S[\mathsf{X}^{\pm 1}],\ m, n \in \mathbb{N},$$

$$\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \ni \textstyle\sum_{i=-n}^{\infty} a_i\mathsf{X}^i \overset{\theta_f^{(4)}}{\longmapsto} \sum_{i=-n}^{\infty} f(a_i)\mathsf{X}^i \in \mathrm{Laur}_S[\![\mathsf{X}^{\pm 1}]\!],\ n \in \mathbb{N},$$

είναι ομομορφισμοί δακτυλίων με $\theta_f^{(j)}(1_R) = 1_S$ και να προσδιορισθούν οι πυρήνες $\mathrm{Ker}(\theta_f^{(j)})$ για κάθε $j \in \{1,2,3,4\}$ (βλ. 1.3.1 και άσκηση **1-43**). Εν συνεχεία, να επαληθευθούν για κάθε $j \in \{1,2,3,4\}$ οι ακόλουθες αμφίπλευρες συνεπαγωγές:

(i) Η $\theta_f^{(j)}$ είναι μονομορφισμός $\Leftrightarrow$ ο f είναι μονομορφισμός.

(ii) Η $\theta_f^{(j)}$ είναι επιμορφισμός $\Leftrightarrow$ ο f είναι επιμορφισμός.

3-39. Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και έστω

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i\mathsf{X}^i \in R[\mathsf{X}].$$

Να αποδειχθεί η ακόλουθη αμφίπλευρη συνεπαγωγή (η οποία γενικεύει το πρώτο αποτέλεσμα τού (iii) τής προτάσεως 1.3.9 που περιγράφει την ομάδα $R[\mathsf{X}]^\times$ στην ειδική περίπτωση όπου ο R είναι *ακεραία περιοχή*):

$$\varphi(\mathsf{X}) \in R[\mathsf{X}]^\times \Longleftrightarrow a_0 \in R^\times \text{ και } a_j \in \mathrm{Nil}(R),\ \forall j \in \{1,\ldots,n\}.$$

[*Υπόδειξη*: Για την κατεύθυνση "$\Leftarrow$" να χρησιμοποιηθούν οι ασκήσεις **2-6** και **1-22**. Για την απόδειξη τής συνεπαγωγής "$\Rightarrow$" να αποδειχθεί απευθείας ότι $a_0 \in R^\times$ και να θεωρηθεί *τυχόν* πρώτο ιδεώδες $\mathfrak{p}$ τού R, ο φυσικός επιμορφισμός $\pi_{\mathfrak{p}}^R : R \longrightarrow R/\mathfrak{p}$ και ο επαγόμενος επιμορφισμός

$$\theta^{(1)}_{\pi_{\mathfrak{p}}^R} : R[\mathsf{X}] \longrightarrow (R/\mathfrak{p})[\mathsf{X}] \text{ με } \theta^{(1)}_{\pi_{\mathfrak{p}}^R}(1_R) = 1_{R/\mathfrak{p}} = 1_R + \mathfrak{p}.$$

(Βλ. άσκηση **3-38**.) Σύμφωνα με το θεώρημα 2.6.4 ο πηλικοδακτύλιος $R/\mathfrak{p}$ είναι ακεραία περιοχή. Ως εκ τούτου, ο $(R/\mathfrak{p})[\mathsf{X}]$ είναι ωσαύτως ακεραία περιοχή (βλ. 1.3.9 (i)). Κατά το (viii) τής προτάσεως 3.1.4,

$$\sum_{i=0}^{n} \pi_{\mathfrak{p}}^R(a_i)\mathsf{X}^i \in ((R/\mathfrak{p})[\mathsf{X}])^\times,$$

οπότε εφαρμόζοντας γι' αυτό το πολυώνυμο το πρώτο αποτέλεσμα τού (iii) τής προτάσεως 1.3.9 λαμβάνουμε

$$\pi_{\mathfrak{p}}^{R}(a_0) \in ((R/\mathfrak{p})[\mathsf{X}])^{\times}, \ \ \pi_{\mathfrak{p}}^{R}(a_j) = 0_{R/\mathfrak{p}} = \mathfrak{p}, \ \forall j \in \{1, \ldots, n\}.$$

Από τις τελευταίες ισότητες έπεται ότι $a_j \in \mathfrak{p}$, $\forall j \in \{1, \ldots, n\}$. Επειδή το $\mathfrak{p}$ είναι αυθαιρέτως επιλεγμένο πρώτο ιδεώδες τού R, συμπεραίνουμε τελικώς ότι

$$a_j \in \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(R)\} = \mathrm{Nil}(R), \ \forall j \in \{1, \ldots, n\},$$

κάνοντας χρήση τού (ii) τής ασκήσεως **2-37**.]

3-40. Να αποδειχθεί ότι για οιονδήποτε δακτύλιο R και οιονδήποτε $n \in \mathbb{N}$ η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R^{\mathrm{opp}}) \ni \mathbf{A} \longmapsto \mathbf{A}^{\intercal} \in (\mathrm{Mat}_{n\times n}(R))^{\mathrm{opp}}$$

είναι ισομορφισμός, όπου R^{opp} είναι ο δακτύλιος ο αντικείμενος τού R (βλ. άσκηση **1-3**) και $\mathbf{A}^{\intercal}$ ο *ανάστροφος* τού πίνακα $\mathbf{A}$ (που προκύπτει από τον $\mathbf{A}$ όταν καθιστούμε τις γραμμές του στήλες (και τις στήλες του γραμμές)).

3-41. Να αποδειχθεί ότι για οιονδήποτε δακτύλιο R με μοναδιαίο στοιχείο και οιονδήποτε $n \in \mathbb{N}$ υφίστανται κανονιστικοί ισομορφισμοί

$$\boxed{\mathrm{Mat}_{n\times n}(R)[\mathsf{X}] \cong \mathrm{Mat}_{n\times n}(R[\mathsf{X}])} \ \text{ και } \ \boxed{\mathrm{Mat}_{n\times n}(R)[\![\mathsf{X}]\!] \cong \mathrm{Mat}_{n\times n}(R[\![\mathsf{X}]\!]).}$$

3-42. Δοθέντος ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ και ενός $n \in \mathbb{N}$ να αποδειχθεί ότι η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R) \ni (a_{jk})_{1\leq j,k\leq n} \overset{\mathrm{Mat}_{n\times n}(f)}{\longmapsto} (f(a_{jk}))_{1\leq j,k\leq n} \in \mathrm{Mat}_{n\times n}(S),$$

είναι ομομορφισμός δακτυλίων και έχει τις εξής ιδιότητες:

(i) Η $\mathrm{Mat}_{n\times n}(f)$ είναι μονομορφισμός $\Leftrightarrow$ ο f είναι μονομορφισμός.

(ii) Η $\mathrm{Mat}_{n\times n}(f)$ είναι επιμορφισμός $\Leftrightarrow$ ο f είναι επιμορφισμός.

3-43. Έστω I ένα ιδεώδες ενός δακτυλίου R. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$ υφίσταται κανονιστικός ισομορφισμός δακτυλίων

$$\boxed{\mathrm{Mat}_{n\times n}(R)\,/\,\mathrm{Mat}_{n\times n}(I) \cong \mathrm{Mat}_{n\times n}(R/I)}$$

[*Υπόδειξη*: Να αποδειχθεί ότι ο επιμορφισμός

$$\mathrm{Mat}_{n\times n}(\pi_I^R) : \mathrm{Mat}_{n\times n}(R) \longrightarrow \mathrm{Mat}_{n\times n}(R/I)$$

(ο ορισθείς στην άσκηση **3-42**) έχει ως πυρήνα του το ιδεώδες $\mathrm{Mat}_{n\times n}(I)$ και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.3.]

3-44. Έστω R τυχών δακτύλιος και έστω n ένας φυσικός αριθμός ≥ 2. Για κάθε n-άδα $(r_1, \ldots, r_n) \in R^n$ σημειώνουμε ως $\mathrm{diag}(r_1, \ldots, r_n)$ τον *διαγώνιο πίνακα* $(a_{jk})_{1 \leq j,k \leq n} \in \mathrm{Mat}_{n \times n}(R)$ με εγγραφές τις

$$a_{jk} := \begin{cases} r_j, & \text{όταν } j = k, \\ 0_R, & \text{όταν } j \neq k. \end{cases}$$

(i) Να αποδειχθεί ότι το σύνολο των διαγωνίων πινάκων

$$\mathrm{Diag}_n(R) := \{ \mathrm{diag}(r_1, \ldots, r_n) \mid (r_1, \ldots, r_n) \in R^n \}$$

είναι ένας υποδακτύλιος τού $\mathrm{Mat}_{n \times n}(R)$ που είναι ισόμορφος με τον R^n.

(ii) Σύμφωνα με την άσκηση **2-18**, ο $\mathrm{SUT}_n(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{UT}_n(R)$ και ο $\mathrm{LUT}_n(R)$ ένα ιδεώδες τού δακτυλίου $\mathrm{LT}_n(R)$. Να αποδειχθεί ότι

$$\mathrm{UT}_n(R)/\mathrm{SUT}_n(R) \cong \mathrm{Diag}_n(R) \cong \mathrm{LT}_n(R)/\mathrm{LUT}_n(R).$$

3-45. Να προσδιορισθούν όλα τα ιδεώδη τού δακτυλίου $\mathrm{Mat}_{n \times n}(\mathbb{Z}_{12})$ $(n \in \mathbb{N})$. [*Υπόδειξη*: Να χρησιμοποιηθεί το εδάφιο 3.2.6 σε συνδυασμό με το (vi) τής ασκήσεως **2-16**.]

3-46. Να προσδιορισθούν τα σύνολα λύσεων των συστημάτων γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{array} \right\}$$

και

$$\left\{ \begin{array}{l} 5x \equiv 6 \pmod{8} \\ 8x \equiv 10 \pmod{14} \\ 10x \equiv 5 \pmod{15} \end{array} \right\}$$

βάσει των τεχνικών που παρετέθησαν στην ενότητα 3.4.

3-47. Έστω m ένας ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθεί ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{m}]) = \mathbb{Q}(\sqrt{m})$. [*Υπόδειξη*: Να γενικευθούν καταλλήλως τα προαναφερθέντα στο παράδειγμα 3.5.10.]

3-48. Έστω R μια ακεραία περιοχή. Να αποδειχθεί ότι $\chi\alpha\rho(\mathbf{Fr}(R)) = \chi\alpha\rho(R)$.

3-49. Να αποδειχθούν τα ακόλουθα:

(i) Έστω K ένα σώμα και έστω K_0 το (μοναδικό) πρώτο υπόσωμα τού K (βλ. θεώρημα 3.6.3). Εάν ο $f : K \longrightarrow K$ είναι ένας αυτομορφισμός τού K, τότε

$$f(a) = a, \ \forall a \in K_0.$$

Εξ αυτού έπεται, ειδικότερα, ότι η ταυτοτική απεικόνιση είναι ο μόνος αυτομορφισμός ενός πρώτου σώματος. [*Υπόδειξη*: Να χρησιμοποιηθεί η παρατήρηση 3.6.6.]

(ii) Δεν υπάρχουν άλλοι αυτομορφισμοί τού σώματος $\mathbb{R}$ των πραγματικών αριθμών πέραν τού ταυτοτικού. [*Υπόδειξη*: Είναι εύκολος ο έλεγχος τού ότι κάθε αυτομορφισμός $f : \mathbb{R} \longrightarrow \mathbb{R}$ τού $\mathbb{R}$ έχει την ιδιότητα: $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ (βάσει τού (i)) και διατηρεί τη συνήθη διάταξη τού $\mathbb{R}$. Να χρησιμοποιηθεί το γεγονός ότι κάθε πραγματικός αριθμός είναι το όριο μιας (συγκλίνουσας) ακολουθίας ρητών αριθμών.]

(iii) Το (ii) δεν είναι αληθές για το σώμα $\mathbb{C}$ και για το στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$. (Αρκεί η παράθεση ενός μη ταυτοτικού αυτομορφισμού για καθέναν εξ αυτών.)

3-50. Έστω R μια ακεραία περιοχή και έστω $\mathfrak{p} \in \mathrm{Spec}(R)$. Το

$$\boxed{R_{\mathfrak{p}} := \left\{ \tfrac{a}{b} \in \mathbf{Fr}(R) \,\middle|\, a \in R, b \in R \smallsetminus \mathfrak{p} \right\}}$$

καλείται **τοπικοποίηση τού** R **στο** $\mathfrak{p}$. Να αποδειχθούν τα εξής:

(i) Το $R_{\mathfrak{p}}$ είναι ένας υποδακτύλιος τού σώματος $\mathbf{Fr}(R)$ περιέχων τον R.

(ii) $\mathbf{Fr}(R) \cong \mathbf{Fr}(R_{\mathfrak{p}})$.

(iii) Ο $R_{\mathfrak{p}}$ είναι τοπικός δακτύλιος έχων το $\mathfrak{m}_{R_{\mathfrak{p}}} := \mathfrak{p}R_{\mathfrak{p}}$ ως το (μοναδικό) μεγιστικό του ιδεώδες.

(iv) $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \mathbf{Fr}(R/\mathfrak{p})$.

(v) Όταν $R = \mathbb{Z}$ και $\mathfrak{p} = \langle p \rangle = p\mathbb{Z}$, όπου p κάποιος πρώτος αριθμός, ο $R_{\mathfrak{p}}$ είναι ο δακτύλιος των p-αδικών κλασμάτων $\mathbb{Z}_{\langle p \rangle}$ ο ορισθείς στην άσκηση **1-11** (σελ. 34) με

$$\mathfrak{m}_{\mathbb{Z}_{\langle p \rangle}} = p\mathbb{Z}_{\langle p \rangle} = \mathbb{Z}_{\langle p \rangle} \smallsetminus \mathbb{Z}_{\langle p \rangle}^{\times} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, \text{μκδ}\,(a,b) = 1 \text{ και } p \nmid b, \ p \mid a \right\}$$

(πρβλ. 2.7.3 (ii)) και $\mathbb{Z}_{\langle p \rangle}/p\mathbb{Z}_{\langle p \rangle} \cong \mathbb{Z}_p$.

ΚΕΦΑΛΑΙΟ 4

Δακτύλιοι που ικανοποιούν συνθήκες αλυσίδων

Στο κεφάλαιο αυτό μελετώνται οι κύριες ιδιότητες δακτυλίων που ικανοποιούν τις λεγόμενες *συνθήκες* (ανιουσών ή κατιουσών) *αλυσίδων*.

$\boxed{4.1}$ ΝΑΙΤΕΡΙΑΝΟΙ ΔΑΚΤΥΛΙΟΙ

4.1.1 Ορισμός. Έστω $\{I_n | n \in \mathbb{N}\}$ ένα αριθμήσιμο σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών ενός δακτυλίου R. Η ακολουθία $\{I_n\}_{n\in\mathbb{N}}$ καλείται **ανιούσα αλυσίδα** αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R όταν ισχύει ο εγκλεισμός $I_n \subseteq I_{n+1}$ για κάθε $n \in \mathbb{N}$. Μια ανιούσα αλυσίδα $\{I_n\}_{n\in\mathbb{N}}$ καλείται **στάσιμη** όταν υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$.

4.1.2 Ορισμός. Λέμε ότι ένας δακτύλιος R ικανοποιεί τη **συνθήκη των ανιουσών αλυσίδων** επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του όταν *κάθε* ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών αυτού είναι στάσιμη.

4.1.3 Θεώρημα. *Έστω R ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Ο R ικανοποιεί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του.*

(ii) *Κάθε μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R περιέχει (τουλάχιστον) ένα μεγιστικό στοιχείο (ως προς τον συνήθη εγκλεισμό).*

ΑΠΟΔΕΙΞΗ. (i)$\Rightarrow$(ii) Έστω $\mathcal{S}$ ένα μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R. Τότε υπάρχει κάποιο στοιχείο, ας το πούμε I_1, εντός τού $\mathcal{S}$. Εάν το I_1 είναι μεγιστικό στοιχείο τού $\mathcal{S}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $I_2 \in \mathcal{S}$, τέτοιο ώστε να ισχύει $I_1 \subseteq I_2$. Εάν το I_2 είναι μεγιστικό στοιχείο τού $\mathcal{S}$, τότε έχει καλώς. Ειδάλλως, θα υπάρχει κάποιο $I_3 \in \mathcal{S}$, τέτοιο ώστε να ισχύει $I_2 \subseteq I_3$. Εφαρμόζοντας κατ' επανάληψιν την ίδια (επαγωγική) συλλογιστική σχηματίζουμε μια ανιούσα αλυσίδα δεξιών (και αντιστοίχως, αριστερών) ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

ανηκόντων στο $\mathcal{S}$, η οποία είναι εξ υποθέσεως στάσιμη, ήτοι υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$. Το αριστερό (και αντιστοίχως, το δεξιό) ιδεώδες I_k είναι μεγιστικό στοιχείο τού $\mathcal{S}$ (βλ. 2.5.13 (i)). Πράγματι· εάν το I είναι οιοδήποτε αριστερό (και αντιστοίχως, οιοδήποτε δεξιό) ιδεώδες ανήκον στο $\mathcal{S}$ για το οποίο ισχύει $I_k \subseteq I$, τότε (λόγω τού τρόπου κατασκευής τής ως άνω αλυσίδας) θα υπάρχει κάποιος $\nu \in \mathbb{N}$ με $I \subseteq I_\nu$, οπότε

$$\left\{ \begin{array}{ll} I \subseteq I_\nu \subseteq I_k, & \text{όταν } \nu \leq k \\ I \subseteq I_\nu = I_k, & \text{όταν } \nu \geq k \end{array} \right\} \Longrightarrow I_k = I.$$

Άρα το I_k είναι όντως μεγιστικό στοιχείο τού $\mathcal{S}$.

(ii)$\Rightarrow$(i) Θεωρούμε *τυχούσα* ανιούσα αλυσίδα

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R. Εξ υποθέσεως, το σύνολο $\{I_n | n \in \mathbb{N}\}$ των μελών αυτής περιέχει κάποιο μεγιστικό στοιχείο, ας πούμε το I_m (ως προς τον συνήθη εγκλεισμό). Για κάθε φυσικό αριθμό $n \geq m$ έχουμε $I_m \subseteq I_n$ (διότι η θεωρηθείσα αλυσίδα είναι ανιούσα), οπότε $I_m = I_n$ (λόγω τού ότι το I_m είναι μεγιστικό στοιχείο τού $\{I_n | n \in \mathbb{N}\}$). Άρα ο R ικανοποιεί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του. □

4.1.4 Ορισμός. Κάθε δακτύλιος R, ο οποίος ικανοποιεί μία (και, ως εκ τούτου, και τις δύο) εκ των συνθηκών (i), (ii) τού θεωρήματος 4.1.3, ονομάζεται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **δακτύλιος τής Noether** ή **εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος**[1]. Ένας δακτύλιος R καλείται

[1] Προς τιμήν τής Emmy Noether (1882-1935), η οποία μελέτησε (περί τη δεκαετία τού 1920) τις ιδιότητες των αλυσίδων ιδεωδών και κατέδειξε τη θεωρητική σημασία τους.

ναιτεριανός δακτύλιος όταν είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών ναιτεριανός. (Προφανώς, για τους *μεταθετικούς* δακτυλίους οι έννοιες «εξ αριστερών ναιτεριανός», «εκ δεξιών ναιτεριανός» και «ναιτεριανός» ταυτίζονται, ενώ για τους *μη μεταθετικούς* δακτυλίους είναι εν γένει διαφορετικές.) Τέλος, κάθε ναιτεριανός δακτύλιος, ο οποίος τυγχάνει να είναι ακεραία περιοχή, ονομάζεται **ναιτεριανή περιοχή**.

4.1.5 Πρόταση. *Εάν η $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος, τότε και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Έστω

$$J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq J_{n+1} \subseteq \cdots \tag{4.1}$$

μια ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού S. Θέτοντας $I_\nu := f^{-1}(J_\nu)$ για κάθε $\nu \in \mathbb{N}$, σχηματίζουμε μια ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών)

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

τού R (βλ. 3.2.1 (ii)). Επειδή ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός, η εν λόγω αλυσίδα είναι *στάσιμη*, ήτοι υπάρχει $k \in \mathbb{N}$ με $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$. Εξάλλου, επειδή εξ υποθέσεως η απεικόνιση f είναι επιρριπτική, έχουμε $J_\nu = f(f^{-1}(J_\nu)) = f(I_\nu)$ για κάθε $\nu \in \mathbb{N}$ (βλ. απόδειξη τού θεωρήματος 3.2.4), οπότε και η αλυσίδα (4.1) είναι κατ' ανάγκην στάσιμη. Ως εκ τούτου, και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός. □

4.1.6 Πόρισμα. *Εάν οι R και S είναι δυο ισόμορφοι δακτύλιοι και ο ένας εξ αυτών εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός, τότε και ο άλλος είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

4.1.7 Πόρισμα. *Έστω R ένας εξ αριστερών (και αντιστοίχως, ένας εκ δεξιών) ναιτεριανός δακτύλιος και έστω I ένα ιδεώδες τού R. Τότε και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τής προτάσεως 4.1.5 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. □

4.1.8 Λήμμα. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι δυο (αριστερά, δεξιά ή αμφίπλευρα) ιδεώδη τού R με*

$$I \subseteq J, \quad I \cap \mathrm{Ker}(f) = J \cap \mathrm{Ker}(f) \ \text{ και } \ f(I) = f(J),$$

τότε $I = J$.

ΑΠΟΔΕΙΞΗ. Αρκεί να αποδειχθεί ότι $J \subseteq I$. Έστω τυχόν στοιχείο $a \in J$. Τότε $f(a) \in f(J) = f(I)$, οπότε υπάρχει κάποιο $b \in I$, τέτοιο ώστε να ισχύει

$$f(a) = f(b) \Longrightarrow f(a-b) = 0_S \Longrightarrow a - b \in \mathrm{Ker}(f).$$

Επειδή $b \in I \subseteq J$, έχουμε

$$a, b \in J \Longrightarrow a - b \in J \Longrightarrow a - b \in J \cap \mathrm{Ker}(f) = I \cap \mathrm{Ker}(f) \subseteq I.$$

Επομένως, $b \in I$ και $a - b \in I \Rightarrow (a-b) + b = a \in I$. Άρα όντως $J \subseteq I$. □

4.1.9 Πρόταση. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν αμφότεροι οι* $\mathrm{Ker}(f)$ *και S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανοί δακτύλιοι, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε *τυχούσα* ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

Εξ υποθέσεως, η ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών

$$I_1 \cap \mathrm{Ker}(f) \subseteq I_2 \cap \mathrm{Ker}(f) \subseteq \cdots \subseteq I_n \cap \mathrm{Ker}(f) \subseteq I_{n+1} \cap \mathrm{Ker}(f) \subseteq \cdots$$

τού $\mathrm{Ker}(f)$ οφείλει να είναι στάσιμη, οπότε

$$\exists \nu \in \mathbb{N} : I_n \cap \mathrm{Ker}(f) = I_\nu \cap \mathrm{Ker}(f)$$

για κάθε φυσικό αριθμό $n \geq \nu$. Κατ' αναλογίαν, η ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού S

$$f(I_1) \subseteq f(I_2) \subseteq \cdots \subseteq f(I_n) \subseteq f(I_{n+1}) \subseteq \cdots$$

οφείλει να είναι στάσιμη, οπότε $\exists \xi \in \mathbb{N} : f(I_n) = f(I_\xi)$ για κάθε φυσικό αριθμό $n \geq \xi$. Θέτοντας $k := \max\{\nu, \xi\}$, παρατηρούμε ότι

$$I_k \subseteq I_n, \quad I_k \cap \mathrm{Ker}(f) = I_n \cap \mathrm{Ker}(f) \text{ και } \ f(I_k) = f(I_n),$$

για κάθε φυσικό αριθμό $n \geq k$. Το προηγηθέν λήμμα 4.1.8 μας πληροφορεί ότι $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$, οπότε και η αρχικώς θεωρηθείσα ανιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R είναι στάσιμη. Αυτό σημαίνει ότι και ο ίδιος ο δακτύλιος R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός. □

4.1.10 Πόρισμα. *Έστω R ένας δακτύλιος. Εάν ένα ιδεώδες αυτού I (ιδωμένο ως «αυτόνομος» δακτύλιος) και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανοί, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός δακτύλιος.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τής προτάσεως 4.1.9 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. □

4.1.11 Θεώρημα. *Για έναν μεταθετικό δακτύλιο R τα ακόλουθα είναι ισοδύναμα:*

(i) *Ο R είναι ναιτεριανός δακτύλιος.*

(ii) *Κάθε ιδεώδες τού R είναι πεπερασμένως παραγόμενο, ήτοι μπορεί να παραχθεί από πεπερασμένου πλήθους στοιχεία τού R.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω I *τυχόν* ιδεώδες τού R. Εάν το I είναι κύριο ιδεώδες, τότε αυτό παράγεται εξ ορισμού από ένα στοιχείο τού R. Στην περίπτωση κατά την οποία $\langle r \rangle \subsetneqq I$ *για κάθε* $r \in I$, θεωρώντας ένα στοιχείο $a_1 \in I$ και ένα στοιχείο $a_2 \in I \setminus \langle a_1 \rangle$ λαμβάνουμε

$$\langle a_1 \rangle \subsetneqq \langle a_1, a_2 \rangle \subseteq I.$$

Εάν $I = \langle a_1, a_2 \rangle$, τότε το I είναι προδήλως πεπερασμένως παραγόμενο. Στην περίπτωση κατά την οποία $\langle a_1, a_2 \rangle \subsetneqq I$, θεωρώντας ένα στοιχείο $a_3 \in I \setminus \langle a_1, a_2 \rangle$ λαμβάνουμε

$$\langle a_1 \rangle \subsetneqq \langle a_1, a_2 \rangle \subsetneqq \langle a_1, a_2, a_3 \rangle \subseteq I.$$

Εάν $I = \langle a_1, a_2, a_3 \rangle$, τότε το I είναι προδήλως πεπερασμένως παραγόμενο. Ειδάλλως, επαναλαμβάνουμε την ίδια διαδικασία θεωρώντας κάποιο $a_4 \in I \setminus \langle a_1, a_2, a_3 \rangle$ κ.ο.κ. Προφανώς, αυτή περατούται ύστερα από πεπερασμένου πλήθους βήματα, ήτοι $\exists k \in \mathbb{N} : I = \langle a_1, \ldots, a_k \rangle$, διότι αλλιώς θα ήταν δυνατόν να κατασκευασθεί μια μη στάσιμη ανιούσα αλυσίδα ιδεωδών τού R

$$\langle a_1 \rangle \subsetneqq \langle a_1, a_2 \rangle \subsetneqq \cdots \subsetneqq \langle a_1, \ldots, a_n \rangle \subsetneqq \langle a_1, \ldots, a_n, a_{n+1} \rangle \subsetneqq \cdots,$$

οπότε θα καταλήγαμε σε αντίφαση.

(ii)⇒(i) Θεωρούμε *τυχούσα* ανιούσα αλυσίδα ιδεωδών τού R

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \tag{4.2}$$

Η ένωση $\bigcup_{n=1}^{\infty} I_n$ είναι ιδεώδες τού δακτυλίου R (βλ. άσκηση **2-5**), οπότε (εξ υποθέσεως) $\exists k \in \mathbb{N}$ και $a_1, \ldots, a_k \in R$, τέτοια ώστε $\bigcup_{n=1}^{\infty} I_n = \langle a_1, \ldots, a_k \rangle$. Επειδή

$$a_1, \ldots, a_k \in \bigcup_{n=1}^{\infty} I_n \Rightarrow [\exists j_1, \ldots, j_k \in \mathbb{N} : a_1 \in I_{j_1}, \ldots, a_k \in I_{j_k}],$$

θέτοντας $\nu := \max\{j_1, \ldots, j_k\}$ λαμβάνουμε

$$a_1, \ldots, a_k \in I_\nu \Longrightarrow \bigcup_{n=1}^{\infty} I_n \subseteq I_\nu.$$

Όμως το I_ν είναι ένα εκ των ιδεωδών που συγκροτούν την αλυσίδα (4.2), οπότε έχουμε την εγκλειστική σχέση $I_\nu \subseteq \bigcup_{n=1}^{\infty} I_n$. Ως εκ τούτου,

$$I_\nu = \bigcup_{n=1}^{\infty} I_n \Rightarrow [I_\nu = I_{\nu+1} = I_{\nu+2} = \cdots] \Rightarrow \text{ η (4.2) είναι στάσιμη}$$

και ο R είναι ναιτεριανός δακτύλιος. □

4.1.12 Παραδείγματα. (i) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών είναι ναιτεριανή περιοχή (βλ. πρόταση 2.2.6).

(ii) Κάθε σώμα είναι προφανώς ναιτεριανή περιοχή (αφού διαθέτει μόνον δύο ιδεώδη, τα οποία είναι κύρια ιδεώδη).

(iii) Ο δακτύλιος

$$\mathcal{C}(\mathbb{R}) := \left\{ f \in \mathbb{R}^{\mathbb{R}} \;\middle|\; f \text{ συνεχής} \right\}$$

δεν είναι ναιτεριανός, διότι θέτοντας $I_n := \left\{ f \in \mathcal{C}(\mathbb{R}) \;:\; f|_{[0,\frac{1}{n}]} = 0 \right\}, \forall n \in \mathbb{N}$, τα I_n είναι ιδεώδη τού $\mathcal{C}(\mathbb{R})$ με

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots$$

(iv) Θεωρούμε τον μη μεταθετικό δακτύλιο

$$R = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \middle| \, a \in \mathbb{Z} \text{ και } b, c \in \mathbb{Q} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{Q}).$$

Θα αποδείξουμε ότι ο R είναι εκ δεξιών ναιτεριανός αλλά δεν είναι εξ αριστερών ναιτεριανός. Το υποσύνολο

$$I = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \in R \, \middle| \, a = c = 0 \text{ και } b \in \mathbb{Q} \right\}$$

αποτελεί (αμφίπλευρο) ιδεώδες τού R, διότι για οιαδήποτε $a \in \mathbb{Z}$ και $b, b', c \in \mathbb{Q}$ έχουμε

$$\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \cdot \left(\begin{array}{cc} 0 & b' \\ 0 & 0 \end{array} \right) = \left(\begin{array}{cc} 0 & ab' \\ 0 & 0 \end{array} \right) \in I$$

και

$$\left(\begin{array}{cc} 0 & b' \\ 0 & 0 \end{array} \right) \cdot \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) = \left(\begin{array}{cc} 0 & b'c \\ 0 & 0 \end{array} \right) \in I.$$

Είναι εύκολο να διαπιστωθεί ότι τα μόνα *δεξιά* ιδεώδη τού R που περιέχονται στο I είναι τα (αμφίπλευρα) ιδεώδη $\{0_R\}$ και I. Άρα το I (ιδωμένο ως «αυτόνομος» δακτύλιος) είναι *εκ δεξιών* ναιτεριανός δακτύλιος. Η απεικόνιση

$$f : R \longrightarrow \mathbb{Z} \times \mathbb{Q}, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) := (a, c),$$

είναι επιμορφισμός δακτυλίων με $\mathrm{Ker}(f) = I$. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.3, $R/I \cong \mathbb{Z} \times \mathbb{Q}$. Επειδή (κατά τα (i) και (ii)) οι $\mathbb{Z}$ και $\mathbb{Q}$ είναι (μεταθετικοί) ναιτεριανοί δακτύλιοι και -ιδιαιτέρως- εκ δεξιών ναιτεριανοί, ο $\mathbb{Z} \times \mathbb{Q}$ είναι εκ δεξιών ναιτεριανός (βλ. άσκηση **4-3**). Κατ' επέκτασιν, και ο πηλικοδακτύλιος R/I είναι εκ δεξιών ναιτεριανός (βλ. πόρισμα 4.1.7). Από το πόρισμα 4.1.10 έπεται ότι και ο ίδιος ο R είναι εκ δεξιών ναιτεριανός. Από την άλλη μεριά, για κάθε $j \in \mathbb{N}$ τα υποσύνολα

$$I_j := \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I \,\middle|\, \exists m \in \mathbb{Z} : b = \frac{m}{2^j} \right\} \subsetneqq R$$

αποτελούν *αριστερά* ιδεώδη τού R, διότι για οιαδήποτε $a, m \in \mathbb{Z}$ και $b, c \in \mathbb{Q}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & \frac{m}{2^j} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{am}{2^j} \\ 0 & 0 \end{pmatrix} \in I_j.$$

Επιπροσθέτως, $I_j \subsetneqq I_{j+1}$, διότι

$$\begin{pmatrix} 0 & \frac{m}{2^j} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{2m}{2^{j+1}} \\ 0 & 0 \end{pmatrix} \in I_{j+1}, \begin{pmatrix} 0 & \frac{1}{2^{j+1}} \\ 0 & 0 \end{pmatrix} \in I_{j+1} \smallsetminus I_j,$$

για κάθε $m \in \mathbb{Z}$ και κάθε $j \in \mathbb{N}$. Κατά συνέπειαν, σχηματίζεται μια *μη στάσιμη* ανιούσα αλυσίδα αριστερών ιδεωδών τού R

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots$$

Αυτό σημαίνει ότι ο R δεν είναι εξ αριστερών ναιτεριανός. (Παρομοίως κατασκευάζεται και ένα παράδειγμα ενός δακτυλίου που είναι εξ αριστερών αλλά όχι και εκ δεξιών ναιτεριανός. Βλ. άσκηση **4-1**.)

4.1.13 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε κάθε ιδεώδες τής τετραγωνικής αριθμητικής περιοχής*

$$\mathbb{Z}[\sqrt{m}] = \left\{ a + b\sqrt{m} \in \mathbb{Z} \;\middle|\; a, b \in \mathbb{Z} \right\} \subsetneqq \mathbb{C}$$

(βλ. άσκηση **1-37**) *μπορεί να παραχθεί από δύο (όχι κατ' ανάγκην διαφορετικά) στοιχεία. (Ως εκ τούτου, η $\mathbb{Z}[\sqrt{m}]$ είναι ναιτεριανή περιοχή.)*

ΑΠΟΔΕΙΞΗ. Έστω I τυχόν ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$. Θέτοντας

$$I_1 := I \cap \mathbb{Z}, \quad I_2 := \left\{ b \in \mathbb{Z} \mid a + b\sqrt{m} \in I, \text{ για κάποιον } a \in \mathbb{Z} \right\},$$

η απόδειξη τής προτάσεως απορρέει από τα ακόλουθα:

(i) Τα I_1 και I_2 είναι ιδεώδη τού $\mathbb{Z}$.

(ii) $I_1 \subseteq I_2$.

(iii) Σύμφωνα με την πρόταση 2.2.6 υπάρχουν $r_1, r_2 \in \mathbb{Z}$, τέτοια ώστε $I_1 = \langle r_1 \rangle$, $I_2 = \langle r_2 \rangle$. Επιπροσθέτως, επειδή $r_2 \in I_2$, υπάρχει κάποιο $c \in \mathbb{Z}$, τέτοιο ώστε $c + r_2\sqrt{m} \in I$. Το I ισούται με

$$I = \left\langle r_1, c + r_2\sqrt{m} \right\rangle = \mathbb{Z}[\sqrt{m}]\, r_1 + \mathbb{Z}[\sqrt{m}]\, \left(c + r_2\sqrt{m}\right). \tag{4.3}$$

Απόδειξη τού (i): Εάν $a_1, a_2 \in I_1$, τότε, επειδή ο $\mathbb{Z}$ είναι δακτύλιος και το I ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$, έχουμε

$$\left.\begin{array}{r} a_1, a_2 \in \mathbb{Z} \Longrightarrow a_1 - a_2 \in \mathbb{Z} \\ a_1, a_2 \in I \Longrightarrow a_1 - a_2 \in I \end{array}\right\} \Longrightarrow a_1 - a_2 \in I_1.$$

Και εάν $k \in \mathbb{Z}$ και $a \in I_1$, τότε, κατ' αναλογίαν,

$$\left.\begin{array}{r} k, a \in \mathbb{Z} \Longrightarrow ka \in \mathbb{Z} \\ k, a \in I \Longrightarrow ka \in I \end{array}\right\} \Longrightarrow ka \in I_1.$$

Άρα το I_1 είναι ιδεώδες τού $\mathbb{Z}$. Από την άλλη μεριά, εάν $b_1, b_2 \in I_2$, τότε υπάρχουν $a_1, a_2 \in \mathbb{Z}$, ούτως ώστε

$$\left.\begin{array}{r} a_1 + b_1\sqrt{m} \in I \\ a_2 + b_2\sqrt{m} \in I \end{array}\right\} \Longrightarrow (a_1 - a_2) + (b_1 - b_2)\sqrt{m} \in I \Longrightarrow b_1 - b_2 \in I_2.$$

Και εάν $k \in \mathbb{Z}$ και $b \in I_2$, τότε υπάρχει $a \in \mathbb{Z}$, ούτως ώστε

$$\left.\begin{array}{r} a + b\sqrt{m} \in I \\ k \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{m}] \end{array}\right\} \Longrightarrow ka + kb\sqrt{m} \in I \Longrightarrow kb \in I_2.$$

Άρα *και* το I_2 είναι ιδεώδες τού $\mathbb{Z}$.

Απόδειξη τού (ii): Για οιοδήποτε $a \in I_1$ έχουμε $a \in \mathbb{Z}$ και $a \in I$. Άρα

$$\left.\begin{array}{r} a \in I \\ \sqrt{m} \in \mathbb{Z}[\sqrt{m}] \end{array}\right\} \Longrightarrow a\sqrt{m} \in I \Longrightarrow a \in I_2.$$

Απόδειξη τού (iii): Κατ' αρχάς παρατηρούμε ότι

$$\left.\begin{array}{r} r_1 \in I_1 \Longrightarrow r_1 \in I \\ c + r_2\sqrt{m} \in I \end{array}\right\} \Longrightarrow \left\langle r_1, c + r_2\sqrt{m} \right\rangle \subseteq I.$$

Έστω τώρα τυχόν $r + s\sqrt{m} \in I$, $r, s \in \mathbb{Z}$. Επειδή $s \in I_2 = \langle r_2 \rangle$, υπάρχει κάποιο στοιχείο $s' \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{m}]$ με $s = s'r_2$. Εξάλλου, επειδή

$$\left.\begin{array}{r} r + s\sqrt{m} \in I \\ s'\left(c + r_2\sqrt{m}\right) \in I \end{array}\right\} \Longrightarrow r + s\sqrt{m} - s'\left(c + r_2\sqrt{m}\right) = r - s'c \in I,$$

και $r - s'c \in \mathbb{Z}$, έχουμε $r - s'c \in I_1 = \langle r_1 \rangle$, οπότε υπάρχει $t \in \mathbb{Z}$, τέτοιο ώστε

$$r - s'c = t\,r_1 \Longrightarrow r = t\,r_1 + s'c.$$

Ως εκ τούτου,

$$r + s\sqrt{m} = t\,r_1 + s'\left(c + r_2\sqrt{m}\right) \in \left\langle r_1, c + r_2\sqrt{m}\right\rangle \Longrightarrow I \subseteq \left\langle r_1, c + r_2\sqrt{m}\right\rangle,$$

οπότε εν τέλει οι ισότητες (4.3) είναι αληθείς. □

4.1.14 Σημείωση. Οι υποδακτύλιοι ναιτεριανών δακτυλίων *δεν* είναι απαραιτήτως ναιτεριανοί. Τούτο έγκειται στο ότι ένα ιδεώδες ενός υποδακτυλίου δεν είναι κατ' ανάγκην ιδεώδες και ολοκλήρου τού δακτυλίου αναφοράς. Επί παραδείγματι, για κάθε $n \in \mathbb{N}$ ορίζεται μια ακεραία συνάρτηση (ήτοι μια ολόμορφη συνάρτηση μιας μεταβλητής ορισμένη επί ολοκλήρου τού $\mathbb{C}$) μέσω τού απειρογινομένου

$$f_n(z) := \pi z \prod_{k=n}^{\infty} \left(1 + \frac{z}{k}\right)\left(1 - \frac{z}{k}\right), \ \forall z \in \mathbb{C},$$

(με $f_1(z) = \sin(\pi z)$), για την οποία ισχύει

$$f_n(z) = 0 \Longleftrightarrow z \in \{0\} \cup \{\pm n, \pm(n+1), \pm(n+2), \ldots\}.$$

Επειδή

$$\langle f_1(z)\rangle \subsetneqq \langle f_2(z)\rangle \subsetneqq \cdots \subsetneqq \langle f_n(z)\rangle \subsetneqq \langle f_{n+1}(z)\rangle \subsetneqq \cdots$$

η ακεραία περιοχή $\mathcal{O}(\mathbb{C})$ είναι μη ναιτεριανός δακτύλιος (βλ. 3.5.6 (iii)), παρότι είναι εμφυτευμένη στο σώμα των κλασμάτων της $\mathcal{M}(\mathbb{C}) := \mathbf{Fr}(\mathcal{O}(\mathbb{C}))$, ήτοι στο σώμα των *μερομόρφων συναρτήσεων* (επί ολοκλήρου τού $\mathbb{C}$), και το $\mathcal{M}(\mathbb{C})$ είναι (προφανώς) ναιτεριανός δακτύλιος.

4.1.15 Θεώρημα. (Θεώρημα Βάσεως τού Hilbert) *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Υποθέτοντας ότι ο $R[\mathsf{X}]$ δεν είναι ναιτεριανός δακτύλιος θα δείξουμε ότι και ο ίδιος ο R δεν είναι ναιτεριανός. Έστω λοιπόν I ένα ιδεώδες τού $R[\mathsf{X}]$ μη πεπερασμένως παραγόμενο. Τότε, εάν

$$\varphi_1(\mathsf{X}) \in I, \ \text{ με } \ \deg(\varphi_1(\mathsf{X})) = \min\left\{ \deg(\varphi(\mathsf{X}))|\, \varphi(\mathsf{X}) \in I \smallsetminus \{0_{R[\mathsf{X}]}\}\right\},$$

μπορούμε να ορίσουμε διαδοχικώς πολυώνυμα:

$$\varphi_{k+1}(\mathsf{X}) \in I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})\rangle,$$

με

$$\deg(\varphi_{k+1}(\mathsf{X})) = \min\{ \deg(\varphi(\mathsf{X}))|\, \varphi(\mathsf{X}) \in I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})\rangle\},$$

για $k = 1, 2, 3, \ldots$, και να θέσουμε $n_k := \deg(\varphi_k(\mathsf{X}))$, $\ R \ni a_k := \mathrm{LC}(\varphi_k(\mathsf{X}))$. Κατ' αυτόν τον τρόπο τού ορισμού των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}), \ldots$ διασφαλίζεται αφ' ενός μεν η ισχύς των ανισοϊσοτήτων

$$n_1 \leq n_2 \leq \cdots \leq n_k \leq n_{k+1} \leq \cdots,$$

αφ' ετέρου δε η ισχύς των ακολούθων εγκλειστικών σχέσεων

$$\langle a_1\rangle \subseteq \langle a_1, a_2\rangle \subseteq \langle a_1, a_2, a_3\rangle \subseteq \cdots \subseteq \langle a_1, \ldots, a_k\rangle \subseteq \langle a_1, \ldots, a_k, a_{k+1}\rangle \subseteq \cdots$$

Θα δείξουμε ότι αυτή η ανιούσα αλυσίδα ιδεωδών τού R δεν είναι στάσιμη. Πράγματι· εάν για κάποιον φυσικό αριθμό k είχαμε

$$\langle a_1, \ldots, a_k\rangle = \langle a_1, \ldots, a_k, a_{k+1}\rangle,$$

τότε το a_{k+1} θα εγράφετο ως

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i, \quad (b_i \in R, \ \forall i, \ 1 \leq i \leq k),$$

οπότε το πολυώνυμο

$$\begin{aligned} I \smallsetminus \langle \varphi_1(\mathsf{X}), \ldots, \varphi_k(\mathsf{X})\rangle \quad &\ni \quad \psi(\mathsf{X}) := \varphi_{k+1}(\mathsf{X}) - \sum_{i=1}^{k} b_i\, \mathsf{X}^{n_{k+1}-n_i}\, \varphi_i(\mathsf{X}) \\ &= \quad (a_{k+1}\mathsf{X}^{n_{k+1}} + \cdots) - \sum_{i=1}^{k} b_i\, \mathsf{X}^{n_{k+1}-n_i}\, (a_i \mathsf{X}^{n_i} + \cdots) \end{aligned}$$

θα είχε βαθμό $\deg(\psi(\mathsf{X})) < \deg\big(\varphi_{k+1}(\mathsf{X})\big)$, πράγμα άτοπο επί τη βάσει τής επιλογής τού $\varphi_{k+1}(\mathsf{X})$. Επομένως, η εν λόγω αλυσίδα ιδεωδών δεν είναι στάσιμη και, ως εκ τούτου, ο R δεν είναι ναιτεριανός δακτύλιος. $\square$

4.1.16 Σημείωση. Η ανωτέρω σύντομη και πολύ κομψή απόδειξη τού θεωρήματος βάσεως τού Hilbert οφείλεται στη μαθηματικό H. Sarges (*Ein Beweis des Hilbertschen Basissatzes*, J. reine ang. Math. **283/284** (1976), 436-437.)

4.1.17 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 4.1.15 και μαθηματική επαγωγή ως προς τον n. □

4.1.18 Θεώρημα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος των επίτυπων δυναμοσειρών $R[\![\mathsf{X}]\!]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Βλ. R.Y. Sharp: *Steps in Commutative Algebra*, second ed., London Mathematical Society, Student Texts, Vol. **51**, Cambridge University Press, 2000, θεώρημα 8.13, σελ. 151-153. (Η απόδειξη ομοιάζει με εκείνην τού θεωρήματος βάσεως 4.1.15 τού Hilbert.) □

4.1.19 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι ναιτεριανός, τότε και ο δακτύλιος $R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το θεώρημα 4.1.18 και μαθηματική επαγωγή ως προς τον n. □

4.2 ΔΑΚΤΥΛΙΟΙ ΚΥΡΙΩΝ ΙΔΕΩΔΩΝ

4.2.1 Ορισμός. Ένας δακτύλιος καλείται **δακτύλιος κυρίων ιδεωδών (=: Δ.Κ.Ι.)** όταν κάθε ιδεώδες του είναι κύριο. Επίσης, κάθε δακτύλιος κυρίων ιδεωδών, ο οποίος τυγχάνει να είναι -ταυτοχρόνως- και ακεραία περιοχή, καλείται **περιοχή κυρίων ιδεωδών (=: Π.Κ.Ι.).**

4.2.2 Πρόταση. *Κάθε Π.Κ.Ι. είναι ναιτεριανή περιοχή.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 4.1.11. □

4.2.3 Πρόταση. *Κάθε σώμα είναι Π.Κ.Ι. και κάθε στρεβλό σώμα Δ.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Τα μόνα ιδεώδη οιουδήποτε στρεβλού σώματος (= διαιρετικού δακτυλίου) είναι το τετριμμένο ιδεώδες και ο εαυτός του (βλ. 2.1.9), τα οποία είναι προφανώς κύρια ιδεώδη. Επιπροσθέτως, επειδή κάθε σώμα είναι ακεραία περιοχή (βλ. 1.2.22), οφείλει να είναι κατ' ανάγκην και Π.Κ.Ι. □

4.2.4 Πρόταση. *Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την πρόταση 2.2.6. $\square$

4.2.5 Πρόταση. *Ας υποθέσουμε ότι ο R είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και η $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν ο R είναι Δ.Κ.Ι., τότε και ο S είναι Δ.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Έστω J τυχόν ιδεώδες τού S. Τότε το ιδεώδες $I = f^{-1}(J)$ είναι κύριο, ας πούμε το $I = \langle a \rangle = Ra$, για κάποιο $a \in R$. Ισχυριζόμαστε ότι

$$J = \langle f(a) \rangle = f(a)S.$$

Πράγματι· εάν $b \in J$, τότε $b = f(c)$ για κάποιο $c \in I$. Εξ αυτού έπεται ότι $c = ra$ για κάποιο $r \in R$, οπότε $b = f(c) = f(ra) = f(r)f(a) \in f(a)S$. Άρα $J = f(a)S$. $\square$

4.2.6 Πόρισμα. *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν ο R είναι Δ.Κ.Ι., τότε και ο πηλικοδακτύλιος R/I, όπου I οιοδήποτε ιδεώδες τού R, είναι Δ.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Αρκεί η εφαρμογή τής προτάσεως 4.2.5 για τον φυσικό επιμορφισμό $\pi_I^R : R \longrightarrow R/I$. $\square$

4.2.7 Πόρισμα. *Εάν $m \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$, τότε ο πηλικοδακτύλιος $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|}$ είναι Π.Κ.Ι., όταν ο $|m|$ είναι πρώτος αριθμός, και Δ.Κ.Ι. (αλλά όχι και Π.Κ.Ι.), όταν ο $|m|$ είναι σύνθετος αριθμός.*

ΑΠΟΔΕΙΞΗ. Προφανής δυνάμει των 1.2.27, 4.2.3, 3.3.4, 2.2.6, καθώς και τού πορίσματος 4.2.6. $\square$

4.2.8 Σημείωση. Μέσω τού πορίσματος 4.2.7 διαπιστώνουμε ότι το 4.2.6 δεν είναι πάντοτε αληθές για περιοχές κυρίων ιδεωδών: Εάν το I είναι ένα μη τετριμμένο ιδεώδες μιας Π.Κ.Ι. R, τότε ο πηλικοδακτύλιος R/I (που είναι Δ.Κ.Ι.) δεν είναι κατ' ανάγκην Π.Κ.Ι.

4.2.9 Παραδείγματα. Στο επόμενο κεφάλαιο θα αποδείξουμε ότι οι δακτύλιοι

$$\mathbb{Z}_{\langle p \rangle} \text{ (p πρώτος, βλ. άσκηση \textbf{1-11})}, \quad K[\mathsf{X}], \; K[\![\mathsf{X}]\!] \text{ (K σώμα)}$$

είναι περιοχές κυρίων ιδεωδών (βλ. εδάφιο 5.4.22).

4.2.10 Ορισμός. Για κάθε $x \in \mathbb{R}$ ορίζονται οι ακέραιοι

$$\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}, \;\; \lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geq x\},$$

και $\{x\} := x - \lfloor x \rfloor$. Ο $\lfloor x \rfloor$ ονομάζεται **το δάπεδο τού** x, ο $\lceil x \rceil$ **η οροφή τού** x και ο $\{x\}$ **το κλασματικό μέρος τού** x. Ο ακέραιος $\{x\}_{\text{εγγ}}$ **ο εγγύτερος τού** x, ορίζεται ως ακολούθως:

$$\{x\}_{\text{εγγ}} := \left\lfloor x + \tfrac{1}{2} \right\rfloor = \left\lceil x - \tfrac{1}{2} \right\rceil.$$

4.2.11 Πρόταση. *Ο δακτύλιος $\mathbb{Z}[i] \subsetneqq \mathbb{C}$ των ακεραίων τού Gauss είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Ο δακτύλιος $\mathbb{Z}[i]$ είναι ακεραία περιοχή (βλ. άσκηση **1-36**). Έστω I ένα ιδεώδες τού $\mathbb{Z}[i]$. Εάν $I = \{0\}$, τότε $I = \langle 0 \rangle$. Εάν $\{0\} \subsetneqq I$, τότε υπάρχει κάποιο $z \in I \smallsetminus \{0\}$. Επιλέγουμε λοιπόν ένα $z_0 \in I \smallsetminus \{0\}$ για το οποίο ισχύει η ισότητα

$$|z_0| := \min\{|z| \mid z \in I \smallsetminus \{0\}\}.$$

Θα αποδείξουμε ότι $I = \langle z_0 \rangle$. Πράγματι· εάν $z_0 = a + bi$, για κάποιους $a, b \in \mathbb{Z}$ (με τουλάχιστον έναν εξ αυτών $\neq 0$), τότε για οιοδήποτε στοιχείο $w = a' + b'i \in I$, $a', b' \in \mathbb{Z}$, το κλάσμα w/z_0 γράφεται ως εξής:

$$\begin{aligned} \frac{w}{z_0} &= \frac{a' + b'i}{a + bi} = \frac{(a' + b'i)(a - bi)}{(a + bi)(a - bi)} \\ &= \frac{(a' + b'i)(a - bi)}{a^2 + b^2} = r + si \in \mathbb{Q}(i) = \mathbf{Fr}(\mathbb{Z}[i]), \end{aligned}$$

όπου $r := \frac{aa' + bb'}{a^2 + b^2} \in \mathbb{Q}$ και $s := \frac{ab' + a'b}{a^2 + b^2} \in \mathbb{Q}$. Θεωρούμε τους «εγγύτερους» ακεραίους $p := \{r\}_{\text{εγγ}}$ και $q := \{s\}_{\text{εγγ}}$ των r και s, αντιστοίχως, οπότε ισχύουν οι ανισοϊσότητες:

$$0 \leq |r - p| \leq \frac{1}{2}, \;\; 0 \leq |s - q| \leq \frac{1}{2},$$

και ορίζουμε ως $\xi := p + qi \in \mathbb{Z}[i]$. Τότε

$$\left| \frac{w}{z_0} - \xi \right| = \sqrt{(r - p)^2 + (s - q)^2} \leq \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{1}{\sqrt{2}} < 1. \tag{4.4}$$

Έστω $\zeta := w - z_0 \xi$. Επειδή $z_0, w \in I$ και $\xi \in \mathbb{Z}[i]$ έχουμε $\zeta \in I$. Ας υποθέσουμε ότι $\zeta \neq 0$. Θέτοντας σε εφαρμογή την (4.4) λαμβάνουμε:

$$|\zeta| = |w - z_0 \xi| = \left| z_0 \left(\frac{w}{z_0} - \xi \right) \right| = |z_0| \left| \frac{w}{z_0} - \xi \right| < |z_0|,$$

πράγμα *άτοπο* λόγω τού αρχικού τρόπου επιλογής τού z_0 (επί τη βάσει τής υποθέσεως περί ελαχίστης απόλυτης τιμής). Συνεπώς,

$$\zeta = 0 \Longrightarrow w = z_0 \xi \Longrightarrow I \subseteq \langle z_0 \rangle .$$

Εξάλλου, $\langle z_0 \rangle = \{ c z_0 \mid c \in \mathbb{Z}[i] \} \subseteq I$. Άρα τελικώς $I = \langle n_0 \rangle$. □

4.2.12 Σημείωση. Γενικότερα, η $\mathbb{Z}[\sqrt{m}]$ είναι Π.Κ.Ι. όταν $m \in \{-2, -1, 2, 3, 6, 7\}$ (βλ. πρόταση 5.4.16 και εδάφιο 5.4.22).

4.2.13 Παράδειγμα. Υπάρχει, βεβαίως, και πληθώρα τετραγωνικών αριθμητικών περιοχών, οι οποίες δεν είναι Π.Κ.Ι. Επί παραδείγματι, η ακεραία περιοχή

$$\mathbb{Z}[\sqrt{-5}] = \{ x + y\sqrt{-5} \mid x, y \in \mathbb{Z} \} \subsetneqq \mathbb{C}$$

δεν είναι Π.Κ.Ι., διότι το $I := \left\langle 2, 1 + \sqrt{-5} \right\rangle$ δεν είναι κύριο ιδεώδες. Πράγματι· υποθέτοντας ότι υπάρχουν κάποιοι $a, b \in \mathbb{Z}$ (με έναν τουλάχιστον εξ αυτών διάφορο τού μηδενός), τέτοιοι ώστε

$$I = \left\langle a + b\sqrt{-5} \right\rangle = \mathbb{Z}[\sqrt{-5}] \left(a + b\sqrt{-5} \right),$$

καταλήγουμε σε κάτι το άτοπο ως ακολούθως: Επειδή $1 + \sqrt{-5} \in I$, θα ισχύει

$$1 + \sqrt{-5} = \left(x + y\sqrt{-5} \right) \left(a + b\sqrt{-5} \right) = (ax - 5y) + (bx + ay)\sqrt{-5},$$

για κάποιους $x, y \in \mathbb{Z}$. Κατά συνέπειαν,

$$\left\{ \begin{array}{l} ax - 5y = 1, \\ bx + ay = 1 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} x = \frac{a+5b}{a^2+5b^2}, \\ y = \frac{a-b}{a^2+5b^2} \end{array} \right\}. \tag{4.5}$$

Διακρίνουμε τρεις περιπτώσεις: (i) $a = b$. Τότε $x = \frac{1}{a}$, και επειδή $x \in \mathbb{Z}$ συνάγουμε ότι $a = \pm 1$, οπότε $a + b\sqrt{-5} = \pm \left(1 + \sqrt{-5} \right)$. Επειδή το 2 ανήκει στο I, θα πρέπει να ισχύει η ισότητα

$$2 = \left(1 + \sqrt{-5} \right) \left(\mu + \nu\sqrt{-5} \right), \tag{4.6}$$

για κάποιους $\mu, \nu \in \mathbb{Z}$. Θεωρώντας τούς συζυγείς και στα δύο μέλη τής (4.6) καταλήγουμε στην

$$2 = \left(1 - \sqrt{-5} \right) \left(\mu - \nu\sqrt{-5} \right). \tag{4.7}$$

Πολλαπλασιάζοντας κατά μέλη τις (4.6) και (4.7) λαμβάνουμε

$$4 = 6 \left(\mu^2 + 5\nu^2 \right). \tag{4.8}$$

Όμως η ισότητα (4.8) είναι αδύνατη, καθότι το δεξιό της μέλος είναι προφανώς > 4, όταν τουλάχιστον ένα εκ των μ, ν είναι διάφορο τού μηδενός, και είναι $= 0$, όταν $\mu = \nu = 0$.

(ii) $a \neq b$ και $b \neq 0$. Σε αυτήν την περίπτωση,

$$1 \leq |a-b| \leq |a| + |b| \leq a^2 + b^2 < a^2 + 5b^2 \Longrightarrow 0 < |y| = \frac{|a-b|}{a^2+5b^2} < 1,$$

(βλ. (4.5)), πράγμα άτοπο, διότι -εξ υποθέσεως- $y \in \mathbb{Z}$.

(iii) $a \neq b$ και $b = 0$. Στην τελευταία αυτή περίπτωση έχουμε (λόγω των (4.5)):

$$\mathbb{Z} \ni x = y = \frac{1}{a} \Longrightarrow a = \pm 1 \Longrightarrow a + b\sqrt{-5} = \pm 1 \Longrightarrow 1 \in I,$$

(οπότε $I = \mathbb{Z}[\sqrt{-5}]$). Τούτο όμως ισοδυναμεί με το ότι

$$1 = 2(\alpha + \sqrt{-5}\beta) + \left(1 + \sqrt{-5}\right)\left(\gamma + \sqrt{-5}\delta\right), \tag{4.9}$$

για κατάλληλους ακεραίους αριθμούς $\alpha, \beta, \gamma, \delta$. Από την (4.9) έπεται ότι

$$\left\{ \begin{array}{l} 2\alpha + \gamma - 5\delta = 1, \\ 2\beta + \gamma + \delta = 0 \end{array} \right\} \Longrightarrow 2\alpha + 10\beta + 6\gamma = 1. \tag{4.10}$$

Αλλά *και* η ισχύς τής (4.10) είναι αδύνατη, καθόσον το αριστερό της μέλος είναι ένας άρτιος και το δεξιό της μέλος ένας περιττός ακέραιος αριθμός.

4.2.14 Παραδείγματα. Άλλα παραδείγματα ανήκοντα στην κλάση των ακεραίων περιοχών που δεν είναι Π.Κ.Ι.: Ο δακτύλιος ο ορισθείς στην άσκηση **2-8**, ο πολυωνυμικός δακτύλιος $\mathbb{Z}[\mathsf{X}]$ (βλ. άσκηση **2-7**) και, γενικότερα, ο $R[\mathsf{X}]$, όπου R μια ακεραία περιοχή που δεν είναι σώμα, οι δακτύλιοι $K[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, $K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!]$ (όπου $n \geq 2$ και K σώμα, βλ. πορίσματα 5.4.25 και 5.4.27) κ.ά.

4.2.15 Πρόταση. *Εάν μια ακεραία περιοχή R είναι Π.Κ.Ι., τότε ένα μη τετριμμένο ιδεώδες της είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.*

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα 2.5.22 κάθε μη τετριμμένο μεγιστικό ιδεώδες τής ακεραίας περιοχής R είναι πρώτο. Έστω τώρα I ένα μη τετριμμένο πρώτο ιδεώδες τής R και έστω J ένα ιδεώδες τής R, για το οποίο ισχύει $I \subsetneqq J \subseteq R$. Επειδή η R είναι Π.Κ.Ι., υπάρχουν $a, b \in R \setminus \{0_R\}$, τέτοια ώστε $I = \langle a \rangle$ και $J = \langle b \rangle$. Επειδή $a \in \langle a \rangle \subsetneqq \langle b \rangle$, υπάρχει κάποιο $c \in R \setminus \{0_R\}$ με $a = bc$. Παρατηρούμε ότι $b \notin \langle a \rangle$ (διότι αλλιώς θα είχαμε $\langle b \rangle \subseteq \langle a \rangle$), οπότε

$$c \in \langle a \rangle \Longrightarrow [\exists d \in R : c = ad] \Longrightarrow a = bc = bad = abd.$$

Καθώς $a \neq 0_R$, αυτό σημαίνει ότι $1_R = bd$ (βλ. πρόταση 1.2.5), οπότε έχουμε $1_R \in \langle b \rangle \Longrightarrow J = R$. Άρα το I είναι μεγιστικό ιδεώδες. □

4.3 ΑΡΤΙΝΙΑΝΟΙ ΔΑΚΤΥΛΙΟΙ

4.3.1 Ορισμός. Έστω $\{I_n | n \in \mathbb{N}\}$ ένα αριθμήσιμο σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών ενός δακτυλίου R. Η ακολουθία $\{I_n\}_{n\in\mathbb{N}}$ καλείται **κατιούσα αλυσίδα** αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R όταν ισχύει ο εγκλεισμός $I_n \supseteq I_{n+1}$ για κάθε $n \in \mathbb{N}$. Μια κατιούσα αλυσίδα $\{I_n\}_{n\in\mathbb{N}}$ καλείται **στάσιμη** όταν υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$.

4.3.2 Ορισμός. Λέμε ότι ένας δακτύλιος R ικανοποιεί τη **συνθήκη των κατιουσών αλυσίδων** επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του όταν *κάθε* κατιούσα αλυσίδα αριστερών (και αντιστοίχως, δεξιών) ιδεωδών αυτού είναι στάσιμη.

Η απόδειξη τού θεωρήματος 4.3.3 είναι παρόμοια εκείνης τού θεωρήματος 4.1.3.

4.3.3 Θεώρημα. *Έστω R ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Ο R ικανοποιεί τη συνθήκη των κατιουσών αλυσίδων επί τού συνόλου των αριστερών (και αντιστοίχως, των δεξιών) ιδεωδών του.*

(ii) *Κάθε μη κενό σύνολο αριστερών (και αντιστοίχως, δεξιών) ιδεωδών τού R περιέχει (τουλάχιστον) ένα ελαχιστικό στοιχείο (ως προς τον συνήθη εγκλεισμό).*

4.3.4 Ορισμός. Κάθε δακτύλιος R, ο οποίος ικανοποιεί μία (και, ως εκ τούτου, και τις δύο) εκ των συνθηκών (i), (ii) τού θεωρήματος 4.3.3, ονομάζεται **εξ αριστερών** (και αντιστοίχως, **εκ δεξιών**) **δακτύλιος τού Artin** ή **εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός δακτύλιος**[2]. Ένας δακτύλιος R καλείται **αρτινιανός δακτύλιος** όταν είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών αρτινιανός. (Προφανώς, για τους *μεταθετικούς* δακτυλίους οι έννοιες «εξ αριστερών αρτινιανός», «εκ δεξιών αρτινιανός» και «αρτινιανός» ταυτίζονται, ενώ για τους *μη μεταθετικούς* δακτυλίους είναι εν γένει διαφορετικές.) Τέλος, κάθε αρτινιανός δακτύλιος, ο οποίος τυγχάνει να είναι ακεραία περιοχή, ονομάζεται **αρτινιανή περιοχή**.

Οι αποδείξεις των προτάσεων 4.3.5 και 4.3.8, και των πορισμάτων 4.3.6 και 4.3.7 είναι παρόμοιες εκείνων των προτάσεων 4.1.5 και 4.1.9, και των πορισμάτων 4.1.6 και 4.1.7, αντιστοίχως.

---

[2]Προς τιμήν τού Emil Artin (1898-1962), ο οποίος μελέτησε ιδιαιτέρως τις ιδιότητες των *κατιουσών* αλυσίδων ιδεωδών.

4.3.5 Πρόταση. *Εάν η $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός δακτύλιος, τότε και ο S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

4.3.6 Πόρισμα. *Εάν οι R και S είναι δυο ισόμορφοι δακτύλιοι και ο ένας εξ αυτών εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός, τότε και ο άλλος είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

4.3.7 Πόρισμα. *Έστω R ένας εξ αριστερών (και αντιστοίχως, ένας εκ δεξιών) αρτινιανός δακτύλιος και έστω I ένα ιδεώδες τού R. Τότε και ο πηλικοδακτύλιος R/I είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

4.3.8 Πρόταση. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν αμφότεροι οι $\mathrm{Ker}(f)$ και S είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανοί δακτύλιοι, τότε και ο ίδιος ο R είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.*

4.3.9 Πρόταση. *Κάθε αρτινιανή περιοχή είναι σώμα.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα αρτινιανή περιοχή. Για οιοδήποτε $r \in R\smallsetminus\{0_R\}$ ισχύουν οι εγκλεισμοί

$$\langle r\rangle \supseteq \langle r^2\rangle \supseteq \langle r^3\rangle \supseteq \cdots \supseteq \langle r^n\rangle \supseteq \langle r^{n+1}\rangle \supseteq \cdots,\ \forall n \in \mathbb{N}.$$

Επειδή η περιοχή R ικανοποιεί τη συνθήκη των κατιουσών αλυσίδων, υπάρχει κάποιος $k \in \mathbb{N}$ για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$. Εξ αυτού έπεται ότι

$$r^k \in \langle r^k\rangle = \langle r^{k+1}\rangle \Rightarrow \exists a \in R : r^k = ar^{k+1},$$

οπότε $\left[r^k(1_R - ar) = 0_R,\ r^k \neq 0_R\right] \Rightarrow ar = 1_R \Rightarrow r \in R^\times$ (βλ. 1.2.5). Κατά συνέπειαν, $R^\times = R\smallsetminus\{0_R\}$ και η R είναι σώμα. □

4.3.10 Παραδείγματα. (i) Κάθε σώμα είναι προφανώς αρτινιανή περιοχή (αφού διαθέτει μόνον δύο κύρια ιδεώδη). Μάλιστα, σύμφωνα με την πρόταση 4.3.9, *ισχύει και το αντίστροφο* (κάτι *που δεν ισχύει* για ναιτεριανές περιοχές)!

(ii) Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο και έστω $n \in \mathbb{N}$. Εάν ο R είναι ναιτεριανός (και αντιστοίχως, αρτινιανός), τότε και ο δακτύλιος $\mathrm{Mat}_{n\times n}(R)$ είναι ναιτεριανός (και αντιστοίχως, αρτινιανός), διότι υφίσταται μια αμφίρριψη μεταξύ τού συνόλου των ιδεωδών τού R και τού συνόλου των ιδεωδών τού $\mathrm{Mat}_{n\times n}(R)$ η οποία διατηρεί τη σχέση εγκλεισμού (βλ. άσκηση **2-16,** (iv) και (vi)). Ιδιαιτέρως, για *κάθε* σώμα K, ο δακτύλιος $\mathrm{Mat}_{n\times n}(K)$ είναι *ταυτοχρόνως* ναιτεριανός και αρτινιανός.

(iii) Στην άσκηση **4-5** δίδεται ένα παράδειγμα ενός δακτυλίου που είναι εκ δεξιών αλλά όχι και εξ αριστερών αρτινιανός.

(iv) Στην άσκηση **4-6** δίδεται ένα παράδειγμα ενός δακτυλίου που είναι εξ αριστερών αλλά όχι και εκ δεξιών αρτινιανός.

(v) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ναιτεριανός (βλ. 4.2.4) αλλά δεν είναι αρτινιανός, διότι η

$$\langle 2\rangle \supsetneqq \langle 4\rangle \supsetneqq \langle 8\rangle \supsetneqq \cdots \supsetneqq \langle 2^n\rangle \supsetneqq \left\langle 2^{n+1}\right\rangle \supsetneqq \cdots, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών του.

(vi) Για οιοδήποτε σώμα K ο δακτύλιος $K[\mathsf{X}]$ είναι ναιτεριανός (σύμφωνα με το θεώρημα 4.1.15) αλλά δεν είναι αρτινιανός, διότι η

$$K[\mathsf{X}] \supsetneqq \langle \mathsf{X}\rangle \supsetneqq \left\langle \mathsf{X}^2\right\rangle \supsetneqq \cdots \supsetneqq \langle \mathsf{X}^n\rangle \supsetneqq \left\langle \mathsf{X}^{n+1}\right\rangle \supsetneqq \cdots, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών του.

(vii) Στην άσκηση **4-8** δίδεται ένα παράδειγμα ενός δακτυλίου που είναι αρτινιανός αλλά δεν είναι ναιτεριανός.

(viii) Εάν για οιονδήποτε θετικό πραγματικό αριθμό ρ θεωρήσουμε το ιδεώδες

$$I_\rho := \left\{ f \in \mathbb{R}^{\mathbb{R}} \middle| \, f(x) = 0 \text{ για κάθε } x \in [-\rho, \rho] \right\}$$

τού δακτυλίου $\mathbb{R}^{\mathbb{R}}$, τότε $\cdots \subsetneqq I_3 \subsetneqq I_2 \subsetneqq I_1 \subsetneqq I_{\frac{1}{2}} \subsetneqq I_{\frac{1}{3}} \subsetneqq I_{\frac{1}{4}} \subsetneqq \cdots$, οπότε η

$$I_1 \subsetneqq I_{\frac{1}{2}} \subsetneqq I_{\frac{1}{3}} \subsetneqq I_{\frac{1}{4}} \subsetneqq \cdots \subsetneqq I_{\frac{1}{n}} \subsetneqq I_{\frac{1}{n+1}}, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη ανιούσα αλυσίδα ιδεωδών και η

$$I_1 \supsetneqq I_2 \supsetneqq I_3 \supsetneqq \cdots \supsetneqq I_n \supsetneqq I_{n+1} \supsetneqq \cdots, \ \forall n \in \mathbb{N}$$

είναι μια μη στάσιμη κατιούσα αλυσίδα ιδεωδών τού $\mathbb{R}^{\mathbb{R}}$. Άρα ο δακτύλιος $\mathbb{R}^{\mathbb{R}}$ δεν είναι ούτε ναιτεριανός ούτε αρτινιανός.

Παρά το γεγονός ότι δεν υφίσταται κάποια αξιομνημόνευτη σχέση διασυνδέσεως *γενικών* ναιτεριανών και αρτινιανών δακτυλίων, τα πράγματα *διαφοροποιούνται* όταν κανείς περιορίζεται *στην κλάση των μεταθετικών δακτυλίων με μοναδιαίο στοιχείο*. Κάθε αρτινιανός μεταθετικός δακτύλιος με μοναδιαίο στοιχείο είναι κατ' ανάγκην ναιτεριανός! Συγκεκριμένα, ισχύει το εξής:

4.3.11 Θεώρημα. (Y. Akizuki & C. Hopkins, 1939) *Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο R είναι αρτινιανός.*

(ii) *Ο R είναι ναιτεριανός και κάθε πρώτο ιδεώδες του είναι μεγιστικό.*

ΑΠΟΔΕΙΞΗ. Βλ., π.χ., I.S. Cohen: *Commutative rings with restricted minimum condition*, Duke Math. Journal **17** (1950), 27-42. □

Ασκήσεις

4-1. Να αποδειχθεί ότι ο (μη μεταθετικός) δακτύλιος

$$R := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix} \right) \middle| \, a, b \in \mathbb{Z} \text{ και } c \in \mathbb{Q} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{Q}).$$

είναι εξ αριστερών ναιτεριανός αλλά δεν είναι εκ δεξιών ναιτεριανός.

4-2. Να αποδειχθεί ότι κάθε ιδεώδες ενός ναιτεριανού δακτυλίου R περιέχει ένα γινόμενο πεπερασμένου πλήθους πρώτων ιδεωδών τού R. [*Υπόδειξη*: Να υποτεθεί ότι το σύνολο των ιδεωδών τού R, τα οποία δεν περιέχουν κανένα γινόμενο πεπερασμένου πλήθους πρώτων ιδεωδών τού R, είναι μη κενό και να χρησιμοποιηθεί εις άτοπον απαγωγή σε συνδυασμό με το θεώρημα 4.1.3.]

4-3. Έστω $n \in \mathbb{N}$, $n \geq 2$. Δοθέντων n δακτυλίων $R_1, \ldots, R_n$, να αποδειχθεί ότι ο δακτύλιος $R_1 \times \cdots \times R_n$ είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός εάν και μόνον εάν καθένας εκ των $R_1, \ldots, R_n$ είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) ναιτεριανός.

4-4. (i) Να αποδειχθεί το θεώρημα 4.3.3.

(ii) Να αποδειχθούν οι προτάσεις 4.3.5 και 4.3.8, και τα πορίσματα 4.3.6 και 4.3.7.

4-5. Να αποδειχθεί ότι ο (μη μεταθετικός) δακτύλιος

$$R := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix} \right) \middle| \, a \in \mathbb{Q} \text{ και } b, c \in \mathbb{R} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

είναι εκ δεξιών αρτινιανός αλλά δεν είναι εξ αριστερών αρτινιανός.

4-6. Να αποδειχθεί ότι ο (μη μεταθετικός) δακτύλιος

$$R := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix} \right) \middle| \, a, b \in \mathbb{R} \text{ και } c \in \mathbb{Q} \right\} \subsetneqq \mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

είναι εξ αριστερών αρτινιανός αλλά δεν είναι εκ δεξιών αρτινιανός.

4-7. Έστω $n \in \mathbb{N}$, $n \geq 2$. Δοθέντων n δακτυλίων $R_1, \ldots, R_n$, να αποδειχθεί ότι ο δακτύλιος $R_1 \times \cdots \times R_n$ είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός εάν και μόνον εάν καθένας εκ των $R_1, \ldots, R_n$ είναι εξ αριστερών (και αντιστοίχως, εκ δεξιών) αρτινιανός.

4-8. Έστω p ένας πρώτος αριθμός και έστω

$$\mathbb{Z}(p^{\infty}) := \left\{ \frac{m}{p^n} \middle| \, n \in \mathbb{N}_0, m \in \mathbb{Z} \text{ και } 0 \leq m < p^n \right\} \subsetneqq \mathbb{Q}.$$

Το σύνολο $\mathbb{Z}(p^{\infty})$ καθίσταται μεταθετικός δακτύλιος (χωρίς μοναδιαίο στοιχείο) μέσω των πράξεων τής προσθέσεως

$$\frac{m}{p^n} + \frac{m'}{p^{n'}} := \begin{cases} \frac{mp^{n'}+m'p^n}{p^{n+n'}}, & \text{όταν } 0 \leq \frac{mp^{n'}+m'p^n}{p^{n+n'}} < 1, \\ \frac{mp^{n'}+m'p^n}{p^{n+n'}} - 1, & \text{όταν } 1 \leq \frac{mp^{n'}+m'p^n}{p^{n+n'}} < 2, \end{cases}$$

για κάθε $n, n' \in \mathbb{N}_0$, $m, m \in \mathbb{Z}$, με $0 \leq m < p^n$, $0 \leq m' < p^{n'}$, και τού τετριμμένου πολλαπλασιασμού

$$ab := 0, \ \forall (a, b) \in \mathbb{Z}(p^{\infty}) \times \mathbb{Z}(p^{\infty}).$$

Να αποδειχθεί ότι αυτός ο δακτύλιος είναι αρτινιανός αλλά δεν είναι ναιτεριανός.

4-9. Έστω $n \in \mathbb{N}$, $n \geq 2$ και έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο ο οποίος περιέχει n ιδεώδη $I_1, \ldots, I_n$, τέτοια ώστε να ισχύει η ισότητα $I_1 \cap \cdots \cap I_n = \{0_R\}$. Υποθέτοντας ότι καθένας εκ των πηλικοδακτυλίων $R/I_1, \ldots, R/I_n$ είναι ναιτεριανός (και αντιστοίχως, αρτινιανός), να αποδειχθεί ότι ο R είναι ωσαύτως ναιτεριανός (και αντιστοίχως, αρτινιανός).

4-10. Έστω R ένας δακτύλιος και έστω $f : R \longrightarrow R$ ένας ενδομορφισμός αυτού. Να αποδειχθούν τα ακόλουθα:

(i) Εάν ο R είναι εκ δεξιών ναιτεριανός και ο f επιμορφισμός, τότε ο f είναι ισομορφισμός. [*Υπόδειξη*: $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f^2)$.]

(ii) Εάν ο R είναι εκ δεξιών αρτινιανός και ο f μονομορφισμός, τότε ο f είναι ισομορφισμός. [*Υπόδειξη*: $\mathrm{Im}(f) \supseteq \mathrm{Im}(f^2)$.]

ΚΕΦΑΛΑΙΟ 5

Θεωρία διαιρετότητας σε ακέραιες περιοχές

Στο πλαίσιο τής Στοιχειώδους Θεωρίας Αριθμών έχουμε μελετήσει τις *ιδιότητες τής διαιρετότητας ακεραίων αριθμών*, τον τρόπο εκτελέσεως τού *ευκλειδείου αλγορίθμου διαιρέσεως*, έχουμε ορίσει τις έννοιες *μέγιστος κοινός διαιρέτης* και *ελάχιστο κοινό πολλαπλάσιο*, και έχουμε αποδείξει ότι κάθε $a \in \mathbb{Z} \setminus \{0\}$ παριστάται ως γινόμενο

$$a = \operatorname{sgn}(a) p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

όπου $\operatorname{sgn}(a)$ είναι ο προσημασμένος άσος τού a (ήτοι $\operatorname{sgn}(a) := 1$, όταν $a > 0$ και $\operatorname{sgn}(a) := -1$, όταν $a < 0$), $k \in \mathbb{N}$, $p_1, \ldots, p_k$ κατάλληλοι σαφώς διακεκριμένοι *πρώτοι αριθμοί* υψούμενοι σε μη αρνητικές ακέραιες δυνάμεις $\alpha_1, \ldots, \alpha_k$. (Η παράσταση αυτή είναι *μονοσημάντως ορισμένη*, μη λαμβανομένης υπ' όψιν τής διατάξεως των $p_1, \ldots, p_k$, για κάθε $a \in \mathbb{Z} \setminus \{0, \pm 1\}$.)

Σκοπός τού παρόντος κεφαλαίου είναι να εξηγήσει το πώς γενικεύονται τα ανωτέρω (που αφορούν στον δακτύλιο $\mathbb{Z}$) σε *τυχούσες ακέραιες περιοχές*. Οι προσήκουσες εννοιολογικές γενικεύσεις, οι οποίες θα εισαχθούν, θα οδηγήσουν στην *ταξινόμηση* των ακεραίων περιοχών επί τη βάσει τής διατηρήσεως ή τής μη διατηρήσεως των θεμελιωδών αριθμοθεωρητικών ή δακτυλιοθεωρητικών ιδιοτήτων τού $\mathbb{Z}$ που οφείλονται -κατά κύριο λόγο- στη *διαιρετότητα*.

5.1 ΑΡΧΙΚΕΣ ΕΠΙΣΗΜΑΝΣΕΙΣ

► **Ευκλείδεια διαίρεση**. Ήδη από τα γραφόμενα στο βιβλίο VII των ευκλειδείων «Στοιχείων» συνάγεται το ακόλουθο:

5.1.1 Θεώρημα. (Η ταυτότητα τής ευκλείδειας διαιρέσεως)
Εάν υποθέσουμε ότι $a \in \mathbb{Z}$ *και ότι* $b \in \mathbb{Z} \smallsetminus \{0\}$, *τότε υπάρχει ένα* μονοσημάντως ορισμένο *ζεύγος* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, *ούτως ώστε*

$$\boxed{a = qb + r, \text{ όπου } 0 \leq r < |b| .} \tag{5.1}$$

Τα q *και* r *στην* (5.1) *είναι το* ***πηλίκο*** *και, αντιστοίχως, το* ***υπόλοιπο*** *τής διαιρέσεως τού* a *διά τού* b.

5.1.2 Σημείωση. Οι ακέραιες περιοχές στις οποίες ορίζεται «ευκλείδεια διαίρεση» (υπό μία κατά τι γενικότερη έννοια) ως προς κάποια «ευκλείδεια στάθμη», καλούνται *ευκλείδειες περιοχές*. (Βλ. τον καταλλήλως τροποποιούμενο ορισμό 5.4.1.) Επισημαίνεται ότι, εν προκειμένω, δεν προαπαιτείται η μοναδικότητα των εμφανιζομένων πηλίκων και υπολοίπων (βλ. 5.4.2 (ii), 5.4.18 και 5.4.19 (ii)). Οι ευκλείδειες περιοχές αποτελούν μια *πολύ ειδική υποκλάση* τής κλάσεως των περιοχών κυρίων ιδεωδών (βλ. θεώρημα 5.4.21).

► **Μέγιστος κοινός διαιρέτης**. Εάν $a, b \in \mathbb{Z}$, τότε, ως συνήθως, γράφουμε $a \mid b$ για να υποδηλώσουμε ότι ο a είναι *διαιρέτης τού* b, δηλαδή ότι υπάρχει κάποιος $c \in \mathbb{Z}$ με $b = ac$. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν οι $a_1, \ldots, a_n$ είναι ακέραιοι αριθμοί με έναν τουλάχιστον εξ αυτών $\neq 0$, τότε το σύνολο $\mathcal{S}$ των θετικών κοινών διαιρετών τους είναι μη κενό, καθότι $1 \in \mathcal{S}$. Επειδή $a_k \neq 0$ για κάποιον $k \in \{1, ..., n\}$, έχουμε $c \mid a_k$ και, ως εκ τούτου, $c \leq |a_k|$, για οιοδήποτε στοιχείο c τού $\mathcal{S}$. Κατά συνέπειαν, το $\mathcal{S}$ είναι πεπερασμένο. Το μέγιστο στοιχείο τού συνόλου $\mathcal{S}$ (ως προς την “ $\leq$ ”) είναι ο *μέγιστος κοινός διαιρέτης* των $a_1, \ldots, a_n$ που τον συμβολίζουμε, ως συνήθως, ως μκδ$(a_1, \ldots, a_n)$. Σημειωτέον ότι για κάθε $a \in \mathbb{Z}$ το σύνολο των θετικών διαιρετών τού a συμπίπτει με το σύνολο των θετικών διαιρετών τού $-a$. Επομένως,

$$\text{μκδ}(a_1, \ldots, a_n) = \text{μκδ}(|a_1|, \ldots, |a_n|),$$

δηλαδή ο μκδ των $a_1, \ldots, a_n$ είναι *ανεξάρτητος* των προσήμων τους. Επίσης, επειδή $a \mid 0$, $\forall a \in \mathbb{Z}$, έχουμε μκδ$(0, a_1, \ldots, a_n) =$ μκδ$(a_1, \ldots, a_n)$. (Σύμβαση: Είναι δυνατή η επέκταση τής εννοίας τού μεγίστου κοινού διαιρέτη ακόμη και όταν $a_1 = \cdots = a_n = 0$. Εν τοιαύτη περιπτώσει, θέτουμε μκδ$(0, \ldots, 0) := 0$.)

5.1.3 Πρόταση. *Εάν* $n \in \mathbb{N}$, $n \geq 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z}$, *τότε ένας* $d \in \mathbb{N}_0$ *ισούται με τον* $\text{μκδ}(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

(i) $d \mid a_1, \ldots, d \mid a_n$,

(ii) *για οιονδήποτε* $c \in \mathbb{Z}$, *για τον οποίο ισχύει* $c \mid a_1, \ldots, c \mid a_n$, *έχουμε* $c \mid d$.

5.1.4 Σημείωση. (i) Στον αρχικό ορισμό τού μεγίστου κοινού διαιρέτη $\text{μκδ}(a_1, \ldots, a_n)$ (όταν τουλάχιστον ένας εκ των $a_1, \ldots, a_n$ είναι $\neq 0$) υπεισέρχεται κατά τρόπο ουσιαστικό η συνήθης διάταξη "$\leq$" των ακεραίων αριθμών. Γι' αυτόν τον λόγο, για να γενικευθεί η έννοια τού μεγίστου κοινού διαιρέτη σε *τυχούσες* ακέραιες περιοχές που δεν είναι κατ' ανάγκην εφοδιασμένες με κάποια σχέση διατάξεως (με το επίθετο *μέγιστος* υπενθυμίζον απλώς την *προέλευση* τού όρου) χρησιμοποιείται μια ελαφρά παραλλαγή[1] τής ανωτέρω προτάσεως 5.1.3 (βλ. ορισμό 5.2.9). Ωστόσο, είναι απαραίτητο να τονισθεί ότι, εν τοιαύτη περιπτώσει, δεν πρέπει να θεωρείται εν γένει ως δεδομένη *ούτε η ύπαρξη* (τέτοιων γενικευμένων) μεγίστων κοινών διαιρετών *ούτε η μοναδικότητά τους* (όταν υπάρχουν).

(ii) Ως γνωστόν, μέσω τής εκτελέσεως πεπερασμένου πλήθους ευκλειδείων διαιρέσεων είναι δυνατός ο προσδιορισμός τού μεγίστου κοινού διαιρέτη $\text{μκδ}(a, b)$ οιωνδήποτε $a, b \in \mathbb{Z} \setminus \{0\}$. Τούτο γενικεύεται καταλλήλως και για οιαδήποτε ευκλείδεια περιοχή (βλ. πρόταση 5.4.28).

► **Ελάχιστο κοινό πολλαπλάσιο**. Έστω ότι $n \in \mathbb{N}$, $n \geq 2$, και ότι οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι αριθμοί. Προφανώς ο φυσικός αριθμός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Ως εκ τούτου, το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ είναι μη κενό και διαθέτει ένα (και μόνον) *ελάχιστο* στοιχείο. Το στοιχείο αυτό είναι το *ελάχιστο κοινό πολλαπλάσιο* των $a_1, \ldots, a_n$ που το συμβολίζουμε, ως συνήθως, ως $\text{εκπ}(a_1, \ldots, a_n)$. Επειδή το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ ισούται με το σύνολο των θετικών πολλαπλασίων των $|a_1|, \ldots, |a_n|$, συμπεραίνουμε ότι $\text{εκπ}(a_1, \ldots, a_n) = \text{εκπ}(|a_1|, \ldots, |a_n|)$. (Σύμβαση: Είναι δυνατή η επέκταση τής εννοίας τού ελαχίστου κοινού πολλαπλασίου ακόμη και όταν τουλάχιστον ένας εκ των $a_1, \ldots, a_n$ είναι $= 0$. Εν τοιαύτη περιπτώσει, θέτουμε $\text{εκπ}(a_1, \ldots, a_n) := 0$.)

5.1.5 Πρόταση. *Εάν* $n \in \mathbb{N}$, $n \geq 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z}$, *τότε ένας* $t \in \mathbb{N}_0$ *ισούται με το* $\text{εκπ}(a_1, \ldots, a_n)$ *εάν και μόνον εάν ισχύουν τα ακόλουθα*:

(i) $a_1 \mid t, \ldots, a_n \mid t$,

(ii) *για οιονδήποτε* $s \in \mathbb{Z}$, *για τον οποίο ισχύει* $a_1 \mid s, \ldots, a_n \mid s$, *έχουμε* $t \mid s$.

[1] Η *ελαφρά παραλλαγή* έγκειται στο ότι ο (γενικευμένος) μέγιστος κοινός διαιρέτης (όταν υπάρχει), δεν υποχρεούται να ανήκει κατ' ανάγκην σε κάποιο *γνήσιο* υποσύνολο τής θεωρούμενης ακεραίας περιοχής.

5.1.6 Σημείωση. Κατ' αναλογίαν προς τα προαναφερθέντα στο εδάφιο 5.1.4 (i), για να γενικευθεί η έννοια τού ελαχίστου κοινού πολλαπλασίου σε *τυχούσες* ακέραιες περιοχές (με το επίθετο *ελάχιστο* υπενθυμίζον απλώς την *προέλευση* τού όρου) χρησιμοποιείται μια ελαφρά παραλλαγή τής ανωτέρω προτάσεως 5.1.5 (βλ. ορισμό 5.2.20). Βεβαίως, *και εδώ* δεν πρέπει να θεωρείται εν γένει ως δεδομένη *ούτε η ύπαρξη* (τέτοιων γενικευμένων) ελαχίστων κοινών πολλαπλασίων *ούτε η μοναδικότητά τους* (όταν υπάρχουν).

► **Ο ρόλος των πρώτων αριθμών**. Οι *πρώτοι αριθμοί* (ήτοι οι ακέραιοι αριθμοί $p \geq 2$ οι έχοντες τους ± 1 και $\pm p$ ως μοναδικούς διαιρέτες τους) αποτελούν τους *δομικούς λίθους* των μη μηδενικών ακεραίων αριθμών υπό την εξής έννοια: Κάθε $a \in \mathbb{Z} \smallsetminus \{0\}$ παρίσταται ως γινόμενο

$$\boxed{a = \mathrm{sgn}(a) p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},} \tag{5.2}$$

όπου $k \in \mathbb{N}$ και $p_1, \ldots, p_k$ κατάλληλοι σαφώς διακεκριμένοι πρώτοι αριθμοί υψούμενοι σε κατάλληλες μη αρνητικές ακέραιες δυνάμεις $\alpha_1, \ldots, \alpha_k$. (Η παράσταση αυτή είναι *μονοσημάντως ορισμένη*, μη λαμβανομένης υπ' όψιν τής διατάξεως των $p_1, \ldots, p_k$, για κάθε $a \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$.) Δύο ικανές και αναγκαίες συνθήκες, υπό τις οποίες η απόλυτη τιμή ενός ακεραίου αριθμού είναι πρώτος αριθμός, δίδονται στις προτάσεις 5.1.7 και 5.1.8.

5.1.7 Πρόταση. *Έστω $n \in \mathbb{Z}$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο $|n|$ είναι πρώτος αριθμός.*

(ii) $n \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ *και για $a, b \in \mathbb{Z}$ ισχύει η συνεπαγωγή:*

$$[n \mid ab \Longrightarrow \text{είτε } n \mid a \text{ είτε } n \mid b].$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή ο $|n|$ είναι πρώτος αριθμός, έχουμε $n \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$. Επιπροσθέτως, εάν $a, b \in \mathbb{Z}$ και $n \mid ab$, τότε υπάρχει κάποιος $k \in \mathbb{Z} : ab = nk$. Στην περίπτωση όπου $ab = 0$, έχουμε είτε $a = 0$ είτε $b = 0$, οπότε $k = 0$ και είτε $n \mid a$ είτε $n \mid b$. Προφανώς, $ab \notin \{\pm 1\}$ (διότι $k \in \mathbb{Z} \smallsetminus \{0\}$ και $|n| \geq 2$). Στην περίπτωση όπου $|ab| \geq 2$, ο $|n|$, όντας πρώτος αριθμός, είναι διαιρέτης τουλάχιστον ενός εκ των $|a|, |b|$, οπότε είτε $n \mid a$ είτε $n \mid b$.

(ii)⇒(i) Εάν $n \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ και εάν θεωρήσουμε τυχόντα $a \in \mathbb{Z} \smallsetminus \{0\}$ που είναι διαιρέτης τού n, τότε υπάρχει κάποιος $b \in \mathbb{Z} \smallsetminus \{0\} : n = ab$. Επειδή $ab = n \cdot 1$, έχουμε $n \mid ab$, οπότε (εξ υποθέσεως) είτε $n \mid a$ είτε $n \mid b$. Εάν $n \mid a$, τότε $|n| = |a|$ και $|b| = 1$, οπότε ο $|n|$ είναι πρώτος αριθμός. Κατ' αναλογίαν, εάν $n \mid b$, τότε $|n| = |b|$ και $|a| = 1$, οπότε ο $|n|$ είναι πρώτος αριθμός. □

5.1.8 Πρόταση. *Έστω $n \in \mathbb{Z}$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο* $|n|$ *είναι πρώτος αριθμός.*

(ii) $n \in \mathbb{Z} \diagdown \{0, \pm 1\}$ *και για* $a, b \in \mathbb{Z}$ *ισχύει η συνεπαγωγή* :

$$[n = ab \Longrightarrow \text{είτε } \; a \in \{\pm 1\} \; \text{ είτε } \; b \in \{\pm 1\}].$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Επειδή ο $|n|$ είναι πρώτος αριθμός, έχουμε $n \in \mathbb{Z} \diagdown \{0, \pm 1\}$. Επιπροσθέτως, εάν $a, b \in \mathbb{Z}$ και $n = ab$, τότε $|n| = |a|\,|b|$, οπότε *είτε* $|n| = |a|$ και $|b| = 1$ ($\Leftrightarrow b \in \{\pm 1\}$) *είτε* $|n| = |b|$ και $|a| = 1$ ($\Leftrightarrow a \in \{\pm 1\}$).

(ii)⇒(i) Εάν $n \in \mathbb{Z} \diagdown \{0, \pm 1\}$ και εάν θεωρήσουμε τυχόντα $a \in \mathbb{Z} \diagdown \{0\}$ που διαιρεί τον n, τότε υπάρχει κάποιος $b \in \mathbb{Z} \diagdown \{0\} \, : \, n = ab$. Εξ υποθέσεως, είτε $a \in \{\pm 1\}$ είτε $b \in \{\pm 1\}$. Εάν $a \in \{\pm 1\}$, τότε $|n| = |b|$ και εάν $b \in \{\pm 1\}$, τότε $|n| = |a|$, οπότε το 1 και ο $|n|$ είναι οι μόνοι θετικοί διαιρέτες τού $|n|$. Αυτό σημαίνει ότι ο $|n|$ είναι πρώτος αριθμός. □

5.1.9 Σημείωση. Για τη γενίκευση τής εννοίας τού πρώτου αριθμού σε *τυχούσες* ακέραιες περιοχές χρησιμοποιούνται *άμεσες* γενικεύσεις αμφοτέρων των συνθηκών 5.1.7 (ii) και 5.1.8 (ii). Αυτές οδηγούν στους ορισμούς των εννοιών *πρώτο στοιχείο* και *ανάγωγο στοιχείο* (βλ. 5.3.1 και 5.3.2, αντιστοίχως). Παρότι οι συνθήκες 5.1.7 (ii) και 5.1.8 (ii) είναι ισοδύναμες στον $\mathbb{Z}$, ένα ανάγωγο στοιχείο μιας ακεραίας περιοχής που δεν είναι Π.Κ.Ι. δεν είναι κατ' ανάγκην πρώτο! (Βλ. 5.3.3 (iv) και 5.3.4 (iii), (iv).)

Δοθέντων n μη μηδενικών ακεραίων αριθμών $a_1, \ldots, a_n$ ($n \in \mathbb{N}$, $n \geq 2$), είναι δυνατόν να δοθούν χρήσιμες εκφράσεις για τον μκδ$(a_1, \ldots, a_n)$ και το εκπ$(a_1, \ldots, a_n)$ μέσω τής παραστάσεως (5.2) καθενός εξ αυτών ως γινομένου πρώτων αριθμών.

5.1.10 Πρόταση. *Εάν* $n \in \mathbb{N}$, $n \geq 2$, *και* $a_1, \ldots, a_n \in \mathbb{Z} \diagdown \{0\}$ *με*

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots, \; |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου οι $p_1, \ldots, p_k$ *είναι σαφώς διακεκριμένοι πρώτοι και οι* $\alpha_{j,l}$, $j \in \{1, ..., n\}$, $l \in \{1, ..., k\}$, *μη αρνητικοί ακέραιοι αριθμοί, τότε*

$$\boxed{\text{μκδ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}} \tag{5.3}$$

και

$$\boxed{\text{εκπ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\max\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.} \tag{5.4}$$

Τέλος, ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο δύο ακεραίων αριθμών συσχετίζονται ως ακολούθως:

5.1.11 Πρόταση. *Για οιουσδήποτε $a, b \in \mathbb{Z}$ έχουμε*

$$\boxed{\text{μκδ}(a,b)\text{εκπ}(a,b) = |ab|\,.} \tag{5.5}$$

5.1.12 Σημείωση. Κατάλληλες γενικεύσεις των (5.3), (5.4) και (5.5) εξακολουθούν να ισχύουν στις λεγόμενες *περιοχές μονοσήμαντης παραγοντοποιήσεως* (βλ. ορισμό 5.6.2, θεώρημα 5.6.11 και πόρισμα 5.6.12).

5.2 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ ΚΑΙ ΙΔΙΟΤΗΤΕΣ

5.2.1 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος.

(i) Έστω $a \in R$. Λέμε ότι το a είναι **διαιρέτης** ενός $b \in R$ (*εντός τού* R και σημειώνουμε[2]: $a \mid b$) όταν υπάρχει κάποιο στοιχείο $x \in R$, τέτοιο ώστε να ισχύει η ισότητα $b = ax$.

(ii) Δυο στοιχεία $a, b \in R$ λέγονται **συντροφικά** (ή **συνεταιρικά**) όταν $a \mid b$ και, ταυτοχρόνως, $b \mid a$. Επίσης, όταν ικανοποιούνται αυτές οι συνθήκες, αναφέρουμε το a ως **σύντροφο** τού b (ή, ισοδυνάμως, λόγω συμμετρίας, το b ως σύντροφο τού a).

5.2.2 Παραδείγματα. (i) Εντός τού δακτυλίου $\mathbb{Z}[i]$ των ακεραίων τού Gauss το στοιχείο $3-4i$ είναι διαιρέτης τού $89-77i$, διότι

$$(3-4i)\,(23+5i) = 89-77i.$$

(ii) Εντός τού δακτυλίου $\mathbb{R}\times\mathbb{Z}$ τού καρτεσιανού γινομένου τού σώματος $\mathbb{R}$ των πραγματικών αριθμών και τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών (βλ. 1.1.4 (v)) ισχύουν οι ισότητες

$$(\sqrt{11}\pi^2, 7)(\sqrt{11}\pi^{-2}, 1) = (11,7)\,, \quad (11,7)\,(11^{-\frac{1}{2}}\pi^2, 1) = (\sqrt{11}\pi^2, 7),$$

(όπου[3] $\pi = 3,14159...$), οπότε τα στοιχεία $(\sqrt{11}\pi^2, 7)$ και $(11,7)$ είναι συντροφικά.

5.2.3 Πρόταση. *Έστω R ένας μεταθετικός δακτύλιος. Τότε ισχύουν τα ακόλουθα:*

(i) $a \mid 0_R$, $\forall a \in R$, *και εάν* $b \in R$ *και* $0_R \mid b$, *τότε* $b = 0_R$.

(ii) *Εάν* $a,\ b \in R$ *και* $a \mid b$, *τότε* $ac \mid bc$, $\forall c \in R$.

(iii) *Εάν* $a, b, c \in R$, *τέτοια ώστε* $a \mid b$ *και* $b \mid c$, *τότε* $a \mid c$.

[2] Κατ' αναλογίαν, όταν το a δεν διαιρεί το b, γράφουμε $a \nmid b$.

[3] $\pi =$ ο λόγος τού μήκους τής περιφέρειας ενός κύκλου προς τη διάμετρό του.

(iv) *Εάν $a, b, c \in R$, τέτοια ώστε $a \mid b$ και $a \mid c$, τότε*[4]

$$a \mid bx + cy, \quad \forall\,(x, y) \in R \times R.$$

(v) *Εάν ο R δεν είναι τετριμμένος δακτύλιος και έχει μοναδιαίο στοιχείο, τότε $a \mid a$, $1_R \mid a$, $\forall a \in R$ και*

$$a \mid 1_R \Longleftrightarrow a \in R^{\times}.$$

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $0_R = 0_R \cdot a$, οπότε $a \mid 0_R$ για κάθε $a \in R$. Και εάν $b \in R$ και $0_R \mid b$, τότε $\exists c \in R : b = c \cdot 0_R = 0_R$.

(ii) Για κάθε $c \in R$ έχουμε

$$a \mid b \Longrightarrow (\exists x \in R : b = ax) \Longrightarrow (\exists x \in R : bc = acx) \Longrightarrow ac \mid bc.$$

(iii) Εάν $a, b, c \in R$, με $a \mid b$ και $b \mid c$, τότε υπάρχουν $x, y \in R$, τέτοια ώστε

$$\left.\begin{array}{r} b = ax \\ c = by \end{array}\right\} \Longrightarrow c = axy \Longrightarrow a \mid c.$$

(iv) Εάν $a, b, c \in R$, με $a \mid b$ και $a \mid c$, τότε υπάρχουν $a', a'' \in R$, τέτοια ώστε για οιαδήποτε $x, y \in R$ να ισχύει

$$\left.\begin{array}{r} b = aa' \\ c = aa'' \end{array}\right\} \Longrightarrow bx + cy = a\,(a'x + a''y) \Longrightarrow a \mid bx + cy.$$

(v) Προφανώς, $a = a \cdot 1_R = 1_R \cdot a$ για κάθε $a \in R$ και

$$a \mid 1_R \Longleftrightarrow \exists x \in R : 1_R = ax,$$

το οποίο, λόγω τής ιδιότητας τής μεταθετικότητας εντός τού R ($ax = xa$) ισοδυναμεί με το ότι $a \in R^{\times}$. $\square$

5.2.4 Πρόταση. *Έστω R ένας μη τετριμμένος μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Εάν $a, b, u \in R$, τότε ισχύουν τα ακόλουθα:*

(i) $a \mid b \Longleftrightarrow \langle b \rangle \subseteq \langle a \rangle$.

(ii) *Τα a και b είναι συντροφικά* $\Longleftrightarrow \langle a \rangle = \langle b \rangle$.

(iii) *Η σχέση $[a \underset{\text{συν.}}{\sim} b \underset{\text{ορσ}}{\Longleftrightarrow}$ τα a και b είναι συντροφικά $]$ αποτελεί μια σχέση ισοδυναμίας επί τού R.*

(iv) $u \underset{\text{συν.}}{\sim} 0_R \Longleftrightarrow u = 0_R$, $u \underset{\text{συν.}}{\sim} 1_R \Longleftrightarrow u \in R^{\times}$ *και*

$$u \in R^{\times} \Longleftrightarrow u \mid r, \quad \forall r \in R$$

(v) *Εάν $a = bx$, όπου $x \in R^{\times}$, τότε τα a και b είναι συντροφικά. Εάν, μάλιστα, ο R είναι ακεραία περιοχή, τότε ισχύει και το αντίστροφο.*

[4] Γενικότερα, εάν $n \in \mathbb{N}$, $b_1, \ldots, b_n \in R$, και $a \mid b_j$ για κάθε $j \in \{1, \ldots, n\}$, τότε (ακολουθώντας την ίδια συλλογιστική) έχουμε $a \mid \sum_{j=1}^{n} x_j b_j$ για οιαδήποτε $x_1, \ldots, x_n \in R$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $a \mid b$, τότε υπάρχει κάποιο $x \in R$ με $b = ax$, οπότε $b \in \langle a \rangle$. Εξάλλου, για οιοδήποτε $c \in \langle b \rangle$ υπάρχει κάποιο y με $c = by$, οπότε

$$c = (ax)\, y = a(xy) \Longrightarrow c \in \langle a \rangle \Longrightarrow \langle b \rangle \subseteq \langle a \rangle .$$

(ii) Προφανώς, τα a και b είναι συντροφικά εάν και μόνον εάν

$$a \mid b \;\text{ και }\; b \mid a \underset{\text{(i)}}{\Longleftrightarrow} \langle b \rangle \subseteq \langle a \rangle \;\text{ και }\; \langle a \rangle \subseteq \langle b \rangle \Longleftrightarrow \langle a \rangle = \langle b \rangle .$$

(iii) Πρόδηλο λόγω τού (ii).

(iv) Η πρώτη αμφίπλευρη συνεπαγωγή έπεται από το (i) και η δεύτερη από το (v) τής προτάσεως 5.2.3. Σε ό,τι αφορά στην τρίτη, εάν το u είναι αντιστρέψιμο, τότε

$$r = u\left(u^{-1} r\right), \;\; \forall r \in R \Longrightarrow u \mid r, \;\; \forall r \in R.$$

Και αντιστρόφως· εάν $u \mid r$ για κάθε $r \in R$, θέτοντας $r = 1_R$ λαμβάνουμε την αμφίπλευρη συνεπαγωγή $u \mid 1_R \Longleftrightarrow u \in R^{\times}$ (βλ. το (v) τής προτάσεως 5.2.3).

(v) Εάν $a = bx$, όπου $x \in R^{\times}$, τότε $b = ax^{-1}$, οπότε $a \underset{\text{συν.}}{\sim} b$. Και αντιστρόφως· εάν ο R είναι ακεραία περιοχή και $a \underset{\text{συν.}}{\sim} b$, τότε υπάρχουν $x, y \in R$, τέτοια ώστε

$$\left.\begin{array}{l} a = bx \\ b = ay \end{array}\right\} \Longrightarrow a = axy,$$

απ' όπου έπεται ότι *είτε* $a = b = 0_R$ (οπότε $0_R = 0_R \cdot u$, $\forall u \in R^{\times}$) *είτε* $1_R = xy$ (βλ. 1.2.5), ήτοι $x, y \in R^{\times}$. □

5.2.5 Πόρισμα. *Για κάθε ζεύγος a, b στοιχείων μιας ακεραίας περιοχής R ισχύει η αμφίπλευρη συνεπαγωγή* :

$$\boxed{a \underset{\text{συν.}}{\sim} b \Longleftrightarrow \left[\exists x \in R^{\times} : a = bx\right].}$$

(Αυτό το x είναι μονοσημάντως ορισμένο *όταν $a, b \in R \smallsetminus \{0_R\}$.)*

ΑΠΟΔΕΙΞΗ. Η ανωτέρω αμφίπλευρη συνεπαγωγή είναι αληθής λόγω τού (v) τής προτάσεως 5.2.4. Όταν τα a, b είναι μη μηδενικά, αυτό το $x \in R^{\times}$ είναι μονοσημάντως ορισμένο λόγω τού κανόνα τής διαγραφής 1.2.5. □

5.2.6 Παραδείγματα. (i) Εντός ενός σώματος K *οιαδήποτε* στοιχεία a, b τού $K \smallsetminus \{0_K\}$ είναι συντροφικά, διότι $a = bb^{-1}a$ και $b^{-1}a \in K^{\times} = K \smallsetminus \{0_K\}$.

(ii) Εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών τα μόνα συντροφικά στοιχεία ενός $n \in \mathbb{Z}$ είναι τα $\pm n$, καθότι $\mathbb{Z}^{\times} = \{\pm 1\}$.

5.2.7 Παρατήρηση. Έστω R μια ακεραία περιοχή. Εάν τα a, b, c, d είναι στοιχεία τής R με $a \underset{\text{συν.}}{\sim} b$ και $c \underset{\text{συν.}}{\sim} d$, τότε $ac \underset{\text{συν.}}{\sim} bd$. (Πράγματι· εάν υπάρχουν $x, y \in R^{\times}$, τέτοια να ισχύουν οι ισότητες $a = bx$ και $c = dy$, τότε $ac = bd(xy)$, όπου $xy \in R^{\times}$.) Ωστόσο, εν γένει *δεν* ισχύει $a+c \underset{\text{συν.}}{\sim} b+d$, όπως διαπιστώνουμε, επί παραδείγματι, όταν $R = \mathbb{Z}[i]$, $a = b = 1$ και $c = 1 + 2i$, $d = -2 + i$. (Πράγματι· $1 \underset{\text{συν.}}{\sim} 1$ και $1 + 2i = i\,(-2 + i)$, οπότε $1 + 2i \underset{\text{συν.}}{\sim} -2 + i$, αλλά τα $2 + 2i$ και $-1 + i$ δεν είναι συντροφικά.)

5.2.8 Σημείωση. Έστω b ένα στοιχείο μιας ακεραίας περιοχής R. Επειδή οι σύντροφοι τού b και τα αντιστρέψιμα στοιχεία τής R είναι *πάντοτε* διαιρέτες τού b, είθισται κάθε $a \in R \smallsetminus R^{\times}$, το οποίο είναι διαιρέτης τού b χωρίς να είναι ταυτοχρόνως και σύντροφός του, να καλείται **γνήσιος διαιρέτης** τού b. (Προφανώς, σύμφωνα με αυτόν τον ορισμό, τα αντιστρέψιμα στοιχεία τής R δεν διαθέτουν κανέναν γνήσιο διαιρέτη, ενώ οι γνήσιοι διαιρέτες τού 0_R είναι τα στοιχεία τού συνόλου $R \smallsetminus (R^{\times} \cup \{0_R\})$.) Βάσει τού (i) τής προτάσεως 5.2.4, *το a είναι γνήσιος διαιρέτης τού b εάν και μόνον εάν* $\langle b \rangle \underset{\neq}{\subsetneq} \langle a \rangle \underset{\neq}{\subsetneq} R$. Επιπροσθέτως, εάν $a, b \in R, c \in R \smallsetminus \{0_R\}$ και $c = ab$, τότε *το στοιχείο a είναι γνήσιος διαιρέτης τού c* $\Longleftrightarrow$ *το b είναι γνήσιος διαιρέτης τού c.* (Τούτο έπεται άμεσα από τις αμφίπλευρες συνεπαγωγές $b \in R^{\times} \Longleftrightarrow a \underset{\text{συν.}}{\sim} c$ και $a \in R^{\times} \Longleftrightarrow b \underset{\text{συν.}}{\sim} c$.)

5.2.9 Ορισμός. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε ένα στοιχείο $d \in R$ καλείται **μέγιστος κοινός διαιρέτης** των $a_1, \ldots, a_n$ όταν ισχύουν τα ακόλουθα:

(i) $d \mid a_1, \ldots, d \mid a_n$,

(ii) για οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, έχουμε $c \mid d$.

Θέτουμε

$$\boxed{\text{ΜΚΔ}_R(a_1, \ldots, a_n) := \left\{ d \in R \;\middle|\; \begin{array}{c} d \text{ μέγιστος κοινός} \\ \text{διαιρέτης των } a_1, \ldots, a_n \end{array} \right\}.}$$

5.2.10 Παραδείγματα. (i) Εάν $a_1, \ldots, a_n \in \mathbb{Z}$, τότε (κάνοντας χρήση τού συνήθους ορισμού τού $\text{μκδ}(a_1, \ldots, a_n)$ τού θεσπιζόμενου εντός τού πλαισίου τής Στοιχειώδους Θεωρίας Αριθμών) διαπιστώνουμε ότι

$$\text{ΜΚΔ}_{\mathbb{Z}}(a_1, \ldots, a_n) = \{\pm \text{μκδ}(a_1, \ldots, a_n)\}.$$

Κατά συνέπειαν, στον $\mathbb{Z}$, από *δακτυλιοθεωρητική σκοπιά* (ήτοι ακολουθώντας τον ορισμό 5.2.9), οι $a_1, \ldots, a_n$ έχουν *αμφότερους* τους $\text{μκδ}(a_1, \ldots, a_n)$ και $-\text{μκδ}(a_1, \ldots, a_n)$ ως μεγίστους κοινούς διαιρέτες τους και

$$\text{μκδ}(a_1, \ldots, a_n) \neq -\text{μκδ}(a_1, \ldots, a_n) \Leftrightarrow \exists j \in \{1, \ldots, n\} : a_j \neq 0.$$

(ii) Θεωρούμε το σύνολο $M = \{1, 2, 3, 4, 5, 6\}$ και το δυναμοσύνολό του $\mathfrak{P}(M)$. Σύμφωνα με την άσκηση **1-7**, η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$ αποτελεί έναν μεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Εάν

$$A_1 = \{2\},\ A_2 = \{2,3\},\ A_3 = \{1,3\},\ B = \{1,2,3\},$$

τότε

$$A_1 \cap B = A_1,\ \ A_2 \cap B = A_2,\ \ A_3 \cap B = A_3 \Longrightarrow B \mid A_j,\ j = 1,2,3.$$

Εξάλλου, οιοδήποτε στοιχείο $C \in \mathfrak{P}(M)$ είναι διαιρέτης των A_j, $j = 1, 2, 3$, οφείλει να περιέχει το B, οπότε

$$B \subseteq C \Longrightarrow B = C \cap B \Longrightarrow C \mid B.$$

Επομένως, $B \in \text{ΜΚΔ}_{\mathfrak{P}(M)}(A_1, A_2, A_3)$.

5.2.11 Σημείωση. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε

(i) το σύνολο $\text{ΜΚΔ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μη κενό (βλ. 5.2.42 (i)),

(ii) το $\text{ΜΚΔ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μονοσύνολο (βλ. 5.2.10 (i)) και

(iii) όταν $\text{ΜΚΔ}_R(a_1, \ldots, a_n) \neq \varnothing$, κάθε μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ είναι *μονοσημάντως ορισμένος μέχρις συντροφικότητας* (ήτοι οιοσδήποτε άλλος μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ οφείλει να είναι σύντροφος αυτού). Τούτο αποδεικνύεται στην επόμενη πρόταση.

5.2.12 Πρόταση. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τού R και $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε ισχύουν τα ακόλουθα:*

(i) *Εάν $d \underset{\text{συν.}}{\sim} d'$, για κάποιο $d' \in R$, τότε $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$.*

(ii) *Εάν $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε $d \underset{\text{συν.}}{\sim} d'$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $d \underset{\text{συν.}}{\sim} d'$, για κάποιο $d' \in R$, τότε

$$\left.\begin{array}{r} d' \mid d \Longrightarrow \exists x \in R : d = d'x \\ \exists a'_j \in R : a_j = da'_j,\ \forall j \in \{1, ..., n\} \end{array}\right\} \Longrightarrow a_j = d'xa'_j,\ \forall j \in \{1, ..., n\},$$

οπότε $d' \mid a_j$ για κάθε $j \in \{1, ..., n\}$. Εξάλλου, για οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, έχουμε $c \mid d$ και κατ' επέκτασιν $c \mid d'$ (αφού εξ υποθέσεως $d \mid d'$, βλ. 5.2.3 (iii)).

(ii) Εάν το $d' \in R$ είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$, τότε λόγω των (i) και (ii) τού ορισμού 5.2.9 ισχύουν οι σχέσεις διαιρετότητας $d \mid d'$ και $d' \mid d$, οπότε $d \underset{\text{συν.}}{\sim} d'$. □

5.2.13 Πόρισμα. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τού R και $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, τότε*

$$d = 0_R \Longleftrightarrow a_1 = \cdots = a_n = 0_R \Longleftrightarrow \text{ΜΚΔ}_R(a_1, \ldots, a_n) = \{0_R\}.$$

Κατά συνέπειαν,

$$d \in R \smallsetminus \{0_R\} \Longleftrightarrow \exists j \in \{1, \ldots, n\} : a_j \in R \smallsetminus \{0_R\}.$$

ΑΠΟΔΕΙΞΗ. Εάν $d = 0_R$, τότε $0_R \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$, οπότε λόγω τού (i) τής προτάσεως 5.2.3 λαμβάνουμε $a_1 = \cdots = a_n = 0_R$. Και αντιστρόφως· εάν ισχύει $a_1 = \cdots = a_n = 0_R$, τότε το 0_R πληροί αμφότερες τις συνθήκες (i) και (ii) τού ορισμού 5.2.9, οπότε $0_R \in \text{ΜΚΔ}_R(0_R, \ldots, 0_R)$. Έστω τυχών $d \in \text{ΜΚΔ}_R(0_R, \ldots, 0_R)$. Τότε $d \underset{\text{συν.}}{\sim} 0_R$ (λόγω τού (ii) τής προτάσεως 5.2.12), οπότε $d = 0_R$ (λόγω τού (iv) τής προτάσεως 5.2.4). □

5.2.14 Θεώρημα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $d, a_1, a_2, \ldots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$ *και*

$$d = r_1a_1 + r_2a_2 + \cdots + r_na_n$$

για κάποια $r_1, r_2, \ldots, r_n \in R$.

(ii) $\langle d \rangle = \langle a_1, a_2, \ldots, a_n \rangle \ (= \langle a_1 \rangle + \langle a_2 \rangle \cdots + \langle a_n \rangle)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ και $d = r_1a_1 + \cdots + r_na_n$ για κάποια $r_1, \ldots, r_n \in R$, τότε προφανώς

$$d \in \langle a_1, a_2, \ldots, a_n \rangle \Longrightarrow \langle d \rangle \subseteq \langle a_1, a_2, \ldots, a_n \rangle.$$

Εξάλλου, για κάθε $j \in \{1, \ldots, n\}$ έχουμε $d \mid a_j \Longrightarrow (\exists x_j \in R : a_j = x_jd)$, οπότε για οιοδήποτε στοιχείο

$$s_1a_1 + s_2a_2 + \cdots + s_na_n \in \langle a_1, a_2, \ldots, a_n \rangle, \ \ s_1, \ldots, s_n \in R,$$

διαπιστώνουμε ότι

$$s_1a_1 + \cdots + s_na_n = (s_1x_1 + \cdots + s_nx_n)\, d \in \langle d \rangle.$$

Άρα τελικώς $\langle d \rangle = \langle a_1, a_2, \ldots, a_n \rangle$.

(ii)⇒(i) Εάν $\langle d \rangle = \langle a_1, a_2, \ldots, a_n \rangle$, τότε προφανώς $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ για κάποια $r_1, r_2, \ldots, r_n \in R$. Επιπροσθέτως, για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$a_j \in \langle d \rangle \Longrightarrow d \mid a_j.$$

Εξάλλου, οιοδήποτε $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, είναι διαιρέτης τού $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ (βλ. 5.2.3 (v)). Άρα το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \ldots, a_n$. □

5.2.15 Πόρισμα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών R με μοναδιαίο στοιχείο, τότε $\text{ΜΚΔ}_R(a_1, \ldots, a_n) \neq \varnothing$, ενώ κάθε $d \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$ παριστάται υπό τη μορφή*

$$\boxed{d = r_1a_1 + r_2a_2 + \cdots + r_na_n,} \tag{5.6}$$

για κάποια $r_1, r_2, \ldots, r_n \in R$.

Αποδειξη. Επειδή ο R είναι Δ.Κ.Ι., υπάρχει κάποιο στοιχείο $d' \in R$, τέτοιο ώστε να ισχύει η ισότητα $\langle d' \rangle = \langle a_1, a_2, \ldots, a_n \rangle$, οπότε το d' γράφεται υπό τη μορφή (5.6). Κατά το θεώρημα 5.2.14 το d' είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \ldots, a_n$. Αλλά και *οιοσδήποτε* μέγιστος κοινός διαιρέτης d των $a_1, a_2, \ldots, a_n$ μπορεί να γραφεί κατ' αυτόν τον τρόπο, αφού $d \underset{\text{συν.}}{\sim} d'$, πράγμα που σημαίνει ότι $\langle d \rangle = \langle d' \rangle$. □

5.2.16 Ορισμός. Έστω ότι $n \in \mathbb{N}$, $n \geq 2$, και ότι τα $a_1, a_2, \ldots, a_n$ είναι μη μηδενικά στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο. Λέμε ότι τα $a_1, a_2, \ldots, a_n$ είναι **σχετικώς πρώτα** (ή ότι είναι **μεταξύ τους πρώτα**) όταν

$$1_R \in \text{ΜΚΔ}_R(a_1, \ldots, a_n).$$

5.2.17 Πόρισμα. (Bézout) *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών R με μοναδιαίο στοιχείο, τότε τα $a_1, a_2, \ldots, a_n$ είναι σχετικώς πρώτα εάν και μόνον εάν*

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 1_R, \tag{5.7}$$

για κάποια $r_1, r_2, \ldots, r_n \in R$, ή -ισοδυνάμως- εάν και μόνον εάν

$$Ra_1 + Ra_2 + \cdots + Ra_n = R.$$

Αποδειξη. Εάν τα $a_1, a_2, \ldots, a_n$ είναι σχετικώς πρώτα, τότε ένας μέγιστος κοινός διαιρέτης τους είναι το 1_R, οπότε ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 5.2.15. Και αντιστρόφως· εάν

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 1_R,$$

για κάποια $r_1, r_2, \ldots, r_n \in R$, τότε για οιοδήποτε στοιχείο $c \in R$, για το οποίο ισχύει $c \mid a_1, \ldots, c \mid a_n$, έχουμε $c \mid 1_R$ (βλ. το (iv) τής προτάσεως 5.2.3). Επειδή προφανώς $1_R \mid a_1, \ldots, 1_R \mid a_n$, συμπεραίνουμε (απευθείας απο τον ορισμό 5.2.9) ότι $1_R \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)$. □

5.2.18 Σημείωση. Εάν ο R δεν είναι Δ.Κ.Ι., τότε οι ισότητες (5.6) και (5.7) δεν ισχύουν πάντοτε. Όταν, π.χ., $R = \mathbb{Z}[\sqrt{-5}]$, τότε τα 2 και $1 + \sqrt{-5}$ είναι σχετικώς πρώτα, χωρίς να υφίσταται ισότητα τής μορφής (5.7). Πράγματι· το 1 είναι (προφανής) διαιρέτης αυτών των στοιχείων. Υποθέτοντας ότι υπάρχουν κάποιοι $a, b \in \mathbb{Z}$ (με τουλάχιστον έναν εξ αυτών διάφορο τού μηδενός), τέτοιοι ώστε

$$a + b\sqrt{-5} \mid 2, \quad a + b\sqrt{-5} \mid 1 + \sqrt{-5},$$

θα υπάρχουν κάποιοι $x, y \in \mathbb{Z}$ με

$$1 + \sqrt{-5} = (x + y\sqrt{-5})(a + b\sqrt{-5}) = (ax - 5y) + (bx + ay)\sqrt{-5},$$

Κατά συνέπειαν,

$$\left\{ \begin{array}{l} ax - 5y = 1, \\ bx + ay = 1 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} x = \frac{a+5b}{a^2+5b^2}, \\ y = \frac{a-b}{a^2+5b^2} \end{array} \right\}. \tag{5.8}$$

Διακρίνουμε τρεις περιπτώσεις: (i) $a = b$. Τότε $x = \frac{1}{a}$, και επειδή $x \in \mathbb{Z}$ συνάγουμε ότι $a = \pm 1$, οπότε

$$a + b\sqrt{-5} = \pm\left(1 + \sqrt{-5}\right).$$

Επειδή αυτό είναι διαιρέτης *και* τού 2, θα πρέπει να ισχύει η ισότητα

$$2 = (1 + \sqrt{-5})(\mu + \nu\sqrt{-5}), \tag{5.9}$$

για κάποιους $\mu, \nu \in \mathbb{Z}$. Θεωρώντας τούς συζυγείς και στα δύο μέλη τής (5.9) καταλήγουμε στην

$$2 = (1 - \sqrt{-5})(\mu - \nu\sqrt{-5}). \tag{5.10}$$

Πολλαπλασιάζοντας κατά μέλη τις (5.9) και (5.10) λαμβάνουμε

$$4 = 6\left(\mu^2 + 5\nu^2\right). \tag{5.11}$$

Όμως η ισχύς τής ως άνω ισότητας (5.11) είναι *αδύνατη*, καθότι το δεξιό της μέλος είναι προφανώς > 4, όταν τουλάχιστον ένα εκ των μ, ν είναι διάφορο τού μηδενός, και είναι $= 0$, όταν $\mu = \nu = 0$.

(ii) $a \neq b$ και $b \neq 0$. Σε αυτήν την περίπτωση,

$$1 \leq |a - b| \leq |a| + |b| \leq a^2 + b^2 < a^2 + 5b^2 \Longrightarrow 0 < |y| = \frac{|a-b|}{a^2 + 5b^2} < 1,$$

(βλ. (5.8)), πράγμα *άτοπο*, διότι -εξ υποθέσεως- $y \in \mathbb{Z}$.

(iii) $a \neq b$ και $b = 0$. Στην τελευταία αυτή περίπτωση έχουμε (λόγω των (5.8)):

$$\mathbb{Z} \ni x = y = \frac{1}{a} \Longrightarrow a = \pm 1 \Longrightarrow a + b\sqrt{-5} = \pm 1,$$

που είναι διαιρέτης τού 1. Άρα οι 2 και $1 + \sqrt{-5}$ είναι όντως *σχετικώς πρώτοι*. Εν συνεχεία, υποθέτοντας ότι υπάρχουν $r_1, r_2 \in \mathbb{Z}[\sqrt{-5}]$, τέτοιοι ώστε να ισχύει η (5.7):

$$2r_1 + \left(1 + \sqrt{-5}\right) r_2 = 1$$

για τα εν λόγω στοιχεία, καταλήγουμε σε *άτοπο*, διότι αυτή ισοδυναμεί με την

$$(1 - \sqrt{-5})(1 + \sqrt{-5})r_1 + 3(1 + \sqrt{-5})r_2 = 3,$$

έχουσα το $1 + \sqrt{-5}$ ως διαιρέτη τού αριστερού της αλλά όχι και τού δεξιού της μέλους! (Στο εδάφιο 4.2.13 είχαμε αποδείξει με ανάλογους συλλογισμούς ότι το ιδεώδες $\left\langle 2, 1 + \sqrt{-5} \right\rangle$ δεν είναι κύριο!)

5.2.19 Πρόταση. *Έστω ότι ο R είναι ένας μεταθετικός δακτύλιος κυρίων ιδεωδών με μοναδιαίο στοιχείο και $a, b, c \in R$. Τότε ισχύουν τα ακόλουθα:*

(i) *Εάν $a \mid bc$ και τα a, b είναι σχετικώς πρώτα, τότε $a \mid c$.*

(ii) *Εάν $a \mid c,\ b \mid c$ και τα a, b είναι σχετικώς πρώτα, τότε $ab \mid c$.*

(iii) *Εάν $c \mid a$ και τα a, b είναι σχετικώς πρώτα, τότε και τα c και b είναι σχετικώς πρώτα.*

ΑΠΟΔΕΙΞΗ. Εάν υποθέσουμε ότι τα a, b είναι σχετικώς πρώτα, τότε, σύμφωνα με το πόρισμα 5.2.17, υπάρχουν $u, v \in R$ με $ua + vb = 1_R$.

(i) Εάν $a \mid bc$, τότε

$$\left. \begin{array}{r} c = uac + vbc \\ a \mid uac,\ a \mid vbc \end{array} \right\} \Longrightarrow a \mid c.$$

(ii) Εάν $a \mid c$ και $b \mid c$, τότε

$$\left. \begin{array}{r} c = uac + vbc \\ ab \mid ac,\ ab \mid bc \end{array} \right\} \Longrightarrow ab \mid c.$$

(iii) Εάν $c \mid a$, τότε $\exists x \in R : a = cx$, οπότε

$$\left. \begin{array}{r} ua + vb = 1_R \\ a = cx \end{array} \right\} \Longrightarrow (ux)\, c + vb = 1_R \Longrightarrow 1_R \in \mathrm{MK\Delta}_R(c, b).$$

(Εν προκειμένω, έγινε χρήση των (ii) και (iv) τής προτάσεως 5.2.3, και τού πορίσματος 5.2.17, αντιστοίχως.) $\square$

5.2.20 Ορισμός. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, και $a_1, \ldots, a_n \in R$, τότε ένα $t \in R$ καλείται **ελάχιστο κοινό πολλαπλάσιο** των $a_1, \ldots, a_n$ όταν ισχύουν τα ακόλουθα:

(i) $a_1 \mid t, \ldots, a_n \mid t$,

(ii) για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \ldots, a_n \mid s$, έχουμε $t \mid s$.

Θέτουμε

$$\boxed{\text{ΕΚΠ}_R(a_1, \ldots, a_n) := \left\{ t \in R \;\middle|\; \begin{array}{c} t \text{ ελάχιστο κοινό} \\ \text{πολλαπλάσιο των } a_1, \ldots, a_n \end{array} \right\}.}$$

5.2.21 Παραδείγματα. (i) Εάν $a_1, \ldots, a_n \in \mathbb{Z}$, τότε (κάνοντας χρήση τού συνήθους ορισμού τού εκπ$(a_1, \ldots, a_n)$ τού θεσπιζόμενου εντός τού πλαισίου τής Στοιχειώδους Θεωρίας Αριθμών) διαπιστώνουμε ότι

$$\text{ΕΚΠ}_{\mathbb{Z}}(a_1, \ldots, a_n) = \{\pm \text{εκπ}(a_1, \ldots, a_n)\}.$$

Κατά συνέπειαν, στον $\mathbb{Z}$, από *δακτυλιοθεωρητική σκοπιά* (ήτοι ακολουθώντας τον ορισμό 5.2.20), οι $a_1, \ldots, a_n$ έχουν *αμφότερα* τα εκπ$(a_1, \ldots, a_n)$ και $-$εκπ$(a_1, \ldots, a_n)$ ως ελάχιστα κοινά πολλαπλάσιά τους και

$$\text{εκπ}(a_1, \ldots, a_n) \neq -\text{εκπ}(a_1, \ldots, a_n) \Leftrightarrow a_j \neq 0, \ \forall j \in \{1, \ldots, n\}.$$

(ii) Θεωρούμε το σύνολο $M = \{1, 2, 3, 4, 5, 6\}$ και το δυναμοσύνολό του $\mathfrak{P}(M)$. Σύμφωνα με την άσκηση **1-7**, η τριάδα $(\mathfrak{P}(M), \triangle, \cap)$ αποτελεί έναν μεταθετικό δακτύλιο με μοναδιαίο στοιχείο. Εάν $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 2, 4\}$, $B_3 = \{1, 2, 3, 4\}$ και $E = \{1, 2\}$, τότε

$$B_1 \cap E = B_2 \cap E = B_2 \cap E = E \Longrightarrow B_j \mid E, \ j = 1, 2, 3.$$

Εξάλλου, οιοδήποτε στοιχείο $C \in \mathfrak{P}(M)$ με τα B_j, $j = 1, 2, 3$, ως διαιρέτες του οφείλει να περιέχεται ταυτοχρόνως στα B_j, $j = 1, 2, 3$, άρα και στην τομή αυτών, οπότε

$$C \subseteq E \Longrightarrow C = C \cap E \Longrightarrow E \mid C.$$

Επομένως, $E \in \text{ΕΚΠ}_{\mathfrak{P}(M)}(B_1, B_2, B_3)$.

5.2.22 Σημείωση. Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, και τα $a_1, \ldots, a_n$ στοιχεία τού R, τότε

(i) το σύνολο $\text{ΕΚΠ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μη κενό (βλ. 5.2.42 (ii)),

(ii) το $\text{ΕΚΠ}_R(a_1, \ldots, a_n)$ δεν είναι κατ' ανάγκην μονοσύνολο (βλ. 5.2.21 (i)) και

(iii) όταν $\text{ΕΚΠ}_R(a_1, \dots, a_n) \neq \varnothing$, κάθε ελάχιστο κοινό πολλαπλάσιο των $a_1, \dots, a_n$ είναι *μονοσημάντως ορισμένο μέχρις συντροφικότητας* (ήτοι οιοδήποτε άλλο ελάχιστο κοινό πολλαπλάσιο των $a_1, \dots, a_n$ οφείλει να είναι σύντροφος αυτού). Τούτο αποδεικνύεται στην επόμενη πρόταση.

5.2.23 Πρόταση. *Εάν ο R είναι ένας μεταθετικός δακτύλιος, $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \dots, a_n$ στοιχεία τού R και $t \in \text{ΕΚΠ}_R(a_1, \dots, a_n)$, τότε ισχύουν τα ακόλουθα:*

(i) *Εάν $t \underset{\text{συν.}}{\sim} t'$, για κάποιο $t' \in R$, τότε $t' \in \text{ΕΚΠ}_R(a_1, \dots, a_n)$.*

(ii) *Εάν το $t' \in \text{ΕΚΠ}_R(a_1, \dots, a_n)$, τότε $t \underset{\text{συν.}}{\sim} t'$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $t \underset{\text{συν.}}{\sim} t'$, για κάποιο $t' \in R$, τότε

$$\left.\begin{array}{r} t \mid t' \Longrightarrow \exists x \in R : t' = tx \\ \exists a_j' \in R : t = a_j a_j', \ \forall j \in \{1, ..., n\} \end{array}\right\} \Longrightarrow t' = a_j a_j' x, \ \forall j \in \{1, ..., n\},$$

οπότε $a_j \mid t'$ για κάθε $j \in \{1, ..., n\}$. Εξάλλου, για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \dots, a_n \mid s$, έχουμε $t \mid s$ και κατ' επέκτασιν $t' \mid s$ (αφού εξ υποθέσεως $t' \mid t$, βλ. 5.2.3 (iii)).

(ii) Εάν το $t' \in R$ είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, \dots, a_n$, τότε λόγω των (i) και (ii) τού ορισμού 5.2.20 ισχύουν οι σχέσεις διαιρετότητας $t \mid t'$ και $t' \mid t$, οπότε $t \underset{\text{συν.}}{\sim} t'$. $\square$

5.2.24 Θεώρημα. *Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $t, a_1, a_2, \dots, a_n$ είναι στοιχεία ενός μεταθετικού δακτυλίου R με μοναδιαίο στοιχείο, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) $t \in \text{ΕΚΠ}_R(a_1, \dots, a_n)$.

(ii) $\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \dots, a_n$, τότε για κάθε $j \in \{1, \dots, n\}$ έχουμε $a_j \mid t$, οπότε

$$t \in \langle a_j \rangle \Longrightarrow t \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle \Longrightarrow \langle t \rangle \subseteq \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle.$$

Από την άλλη μεριά, εάν $r \in \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle$, τότε $r \in \langle a_j \rangle \Longrightarrow a_j \mid r$ για κάθε $j \in \{1, \dots, n\}$, και επειδή το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \dots, a_n$, έχουμε $t \mid r \Longrightarrow r \in \langle t \rangle$, οπότε $\langle a_1 \rangle \cap \dots \cap \langle a_n \rangle \subseteq \langle t \rangle$. Κατά συνέπειαν,

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \dots \cap \langle a_n \rangle.$$

(ii)⇒(i) Εάν υποθέσουμε ότι $\langle t\rangle = \langle a_1\rangle \cap \cdots \cap \langle a_n\rangle$, τότε για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\langle t\rangle \subseteq \langle a_j\rangle \Longrightarrow a_j \mid t,$$

ενώ για οιοδήποτε $s \in R$, για το οποίο ισχύει $a_1 \mid s, \ldots, a_n \mid s$, έχουμε

$$s \in \langle a_j\rangle, \ \forall j \in \{1, \ldots, n\} \Longrightarrow s \in \langle a_1\rangle \cap \cdots \cap \langle a_n\rangle = \langle t\rangle \Longrightarrow t \mid s.$$

Ως εκ τούτου, το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$. □

5.2.25 Πόρισμα. *Οιαδήποτε πεπερασμένου πλήθους στοιχεία ενός μεταθετικού δακτυλίου κυρίων ιδεωδών R με μοναδιαίο στοιχείο διαθέτουν πάντοτε (κάποιο) ελάχιστο κοινό πολλαπλάσιο.*

5.2.26 Πόρισμα. *Έστω R μια ακεραία περιοχή. Εάν $n \in \mathbb{N}$, $n \geq 2$, τα $a_1, \ldots, a_n$ στοιχεία τής R και $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε*

$$t = 0_R \Longleftrightarrow \exists j \in \{1, \ldots, n\} : a_j = 0_R \Longleftrightarrow \text{ΕΚΠ}_R(a_1, \ldots, a_n) = \{0_R\}.$$

Κατά συνέπειαν,

$$t \in R \smallsetminus \{0_R\} \Longleftrightarrow a_j \in R \smallsetminus \{0_R\}, \ \forall j \in \{1, \ldots, n\}.$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $a_j \neq 0_R$ για κάθε $j \in \{1, \ldots, n\}$. Επειδή ο θεωρηθείς δακτύλιος R είναι (εξ υποθέσεως) ακεραία περιοχή, έχουμε $\prod_{j=1}^n a_j \neq 0_R$. Κατά το θεώρημα 5.2.24,

$$\langle t\rangle = \langle a_1\rangle \cap \cdots \cap \langle a_n\rangle.$$

Παρατηρούμε ότι

$$0_R \neq \prod_{j=1}^n a_j \in \langle a_1\rangle \cap \langle a_2\rangle \cap \cdots \cap \langle a_n\rangle = \langle t\rangle \Rightarrow \{0_R\} \subsetneqq \langle t\rangle \Rightarrow t \neq 0_R.$$

Εάν λοιπόν $t = 0_R$, τότε υπάρχει κατ' ανάγκην κάποιος $j \in \{1, \ldots, n\}$ με $a_j = 0_R$. Και αντιστρόφως· εάν $\exists j \in \{1, \ldots, n\} : a_j = 0_R$ και $t \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)$, τότε το θεώρημα 5.2.24 μας πληροφορεί ότι

$$t \in \langle t\rangle \, (= \langle a_1\rangle \cap \langle a_2\rangle \cap \cdots \cap \langle a_n\rangle) \subseteq \langle a_j\rangle = \langle 0_R\rangle = \{0_R\},$$

οπότε $t = 0_R$. □

5.2.27 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν $a, b \in R \smallsetminus \{0_R\}$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Τα a, b είναι σχετικώς πρώτα.*

(ii) *Για κάθε $c \in R \smallsetminus \{0_R\}$ με $c \mid a$ και $c \mid b$, έχουμε $c \in R^{\times}$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $c \in R \smallsetminus \{0_R\}$ και $c \mid a$, $c \mid b$, τότε $c \mid 1_R$ (επειδή εξ υποθέσεως $1_R \in \text{ΜΚΔ}_R(a, b)$, βλ. 5.2.9). Αυτό σημαίνει ότι $\exists c' \in R : 1_R = cc'$, απ' όπου έπεται ότι $c \in R^{\times}$.

(ii)⇒(i) Έστω $c \in R$ με $c \mid a$ και $c \mid b$. Επειδή $a, b \in R \smallsetminus \{0_R\}$, έχουμε κατ' ανάγκην $c \in R \smallsetminus \{0_R\}$ (βλ. 5.2.3 (i)). Εξ υποθέσεως, $c \in R^{\times}$. Αυτό σημαίνει ότι $\exists c' \in R : 1_R = cc'$, απ' όπου έπεται ότι

$$\left.\begin{array}{r} c \mid 1_R \\ \text{5.2.3 (v)} \Rightarrow 1_R \mid a,\ 1_R \mid b \end{array}\right\} \underset{\text{5.2.9}}{\Longrightarrow} 1_R \in \text{ΜΚΔ}_R(a, b),$$

οπότε τα a, b είναι σχετικώς πρώτα. □

5.2.28 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν (κάποιον) μέγιστο κοινό διαιρέτη, τότε για $a, b, d \in R \smallsetminus \{0_R\}$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $d \in \text{ΜΚΔ}_R(a, b)$.

(ii) *Υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $d \in \text{ΜΚΔ}_R(a, b)$, τότε $d \mid a$ και $d \mid b$, οπότε υπάρχουν $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$. Θα αποδείξουμε ότι τα a', b' είναι σχετικώς πρώτα. Προς τούτο θεωρούμε $c \in R$, τέτοιο ώστε $c \mid a'$ και $c \mid b'$. Τότε υπάρχουν $a'', b'' \in R \smallsetminus \{0_R\}$ με $a' = ca''$ και $b' = cb''$. Επομένως,

$$\left.\begin{array}{r} a = dca'' \Rightarrow dc \mid a \\ b = dcb'' \Rightarrow dc \mid b \end{array}\right\} \Longrightarrow dc \mid d \Longrightarrow \exists c' \in R : d = dcc'.$$

Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, έχουμε

$$\left.\begin{array}{r} d(1_R - cc') = 0_R \\ d \neq 0_R \end{array}\right\} \Longrightarrow cc' = 1_R \Rightarrow c \in R^{\times}$$

(βλ. 1.2.5), οπότε $1_R \in \text{ΜΚΔ}_R(a', b')$ (κατόπιν εφαρμογής τού λήμματος 5.2.27 με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως).

(ii)⇒(i) Εξ υποθέσεως, υπάρχει κάποιος $d' \in \text{ΜΚΔ}_R(a, b)$. Επιπροσθέτως, υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$ και $d \in R \smallsetminus \{0_R\}$, τέτοια ώστε

$a = da'$ και $b = db'$. Κατά συνέπειαν,

$$\left.\begin{array}{r} d \mid a \\ d \mid b \end{array}\right\} \underset{5.2.9}{\Longrightarrow} d \mid d' \Rightarrow \exists c \in R \smallsetminus \{0_R\} : d' = dc.$$

Εξάλλου,

$$\left.\begin{array}{r} d' \mid a \Rightarrow \exists a'' \in R \smallsetminus \{0_R\} : da' = a = d'a'' = dca'' \\ d' \mid b \Rightarrow \exists b'' \in R \smallsetminus \{0_R\} : db' = b = d'b'' = dcb'' \\ d \neq 0_R \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a' = ca'' \\ b' = cb'' \end{array}\right\}$$

(βλ. 1.2.5), οπότε εφαρμόζοντας το λήμμα 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως) λαμβάνουμε

$$\left.\begin{array}{r} c \mid a',\ c \mid b' \\ 1_R \in \text{ΜΚΔ}_R(a', b') \end{array}\right\} \Longrightarrow c \in R^{\times}.$$

Από αυτό και από το πόρισμα 5.2.5 συνάγουμε ότι $d' \underset{\text{συν.}}{\sim} d$. Το (i) τής προτάσεως 5.2.12 μας πληροφορεί ότι $d \in \text{ΜΚΔ}_R(a, b)$. □

5.2.29 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν (κάποιο) ελάχιστο κοινό πολλαπλάσιο, τότε για $a, b, t \in R \smallsetminus \{0_R\}$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $t \in \text{ΕΚΠ}_R(a, b)$.

(ii) *Υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε να ισχύουν οι ισότητες $t = aa' = bb'$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $t \in \text{ΕΚΠ}_R(a, b)$, τότε $a \mid t$ και $b \mid t$, οπότε υπάρχουν $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε $t = aa' = bb'$. Θα αποδείξουμε ότι τα a', b' είναι σχετικώς πρώτα στοιχεία. Προς τούτο θεωρούμε τυχόν $c \in R$ με $c \mid a'$ και $c \mid b'$. Λόγω αυτής τής επιλογής τού c υπάρχουν $x, y \in R$, τέτοια ώστε $a' = cx$ και $b' = cy$. Επειδή $a', b' \in R \smallsetminus \{0_R\}$, έχουμε κατ' ανάγκην $c, x, y \in R \smallsetminus \{0_R\}$. Επομένως,

$$\left.\begin{array}{r} t = c(ax) = c(by) \\ c \neq 0_R \end{array}\right\} \Longrightarrow ax = by$$

(βλ. 1.2.5), οπότε

$$\left.\begin{array}{r} a \mid ax \\ b \mid by = ax \end{array}\right\} \underset{5.2.20}{\Longrightarrow} t \mid ax \ \text{ και } \ t = c(ax) \Rightarrow ax \mid t.$$

Επομένως, $t \underset{\text{συν.}}{\sim} ax$ και $c \in R^{\times}$ (βλ. ορισμό 5.2.1 (ii) και πόρισμα 5.2.5). Εφαρμόζοντας το λήμμα 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως) λαμβάνουμε $1_R \in \text{ΜΚΔ}_R(a', b')$.

(ii)⇒(i) Εξ υποθέσεως, υπάρχει κάποιο $t' \in \text{ΕΚΠ}_R(a,b)$. Επιπροσθέτως, υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$ και $t \in R \smallsetminus \{0_R\}$, τέτοια ώστε να ισχύουν οι ισότητες

$$t = aa' = bb'.$$

Κατά συνέπειαν,

$$\left. \begin{array}{c} a \mid t \\ b \mid t \end{array} \right\} \underset{5.2.20}{\Longrightarrow} t' \mid t \Rightarrow \exists c \in R \smallsetminus \{0_R\} : t = t'c.$$

Εξάλλου,

$$\left. \begin{array}{r} a \mid t' \Rightarrow \exists a'' \in R \smallsetminus \{0_R\} : t' = aa'' \\ b \mid t' \Rightarrow \exists b'' \in R \smallsetminus \{0_R\} : t' = bb'' \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} aa' = t = aa''c \\ bb' = t = bb''c \end{array} \right\}.$$

Επειδή $a, b \in R \smallsetminus \{0_R\}$, έχουμε λόγω τής προτάσεως 1.2.5 και τού λήμματος 5.2.27 (με τα a', b' στη θέση των εκεί παρατεθέντων a και b, αντιστοίχως)

$$\left. \begin{array}{c} a' = a''c \Rightarrow c \mid a' \\ b' = b''c \Rightarrow c \mid b' \\ 1_R \in \text{ΜΚΔ}_R(a', b') \end{array} \right\} \Longrightarrow c \in R^{\times}.$$

Από αυτό και από το πόρισμα 5.2.5 συνάγουμε τη σχέση συντροφικότητας $t \underset{\text{συν.}}{\sim} t'$. Το (i) τής προτάσεως 5.2.23 μας πληροφορεί ότι $t \in \text{ΕΚΠ}_R(a,b)$. □

5.2.30 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα εξής:*

(i) *Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη και εάν θεωρήσουμε $a, b \in R \smallsetminus \{0_R\}$, τότε υπάρχει $t \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει*

$$t \in \text{ΕΚΠ}_R(a,b) \ \text{ και } \ td = ab, \ \text{όπου} \ \ d \in \text{ΜΚΔ}_R(a,b).$$

(ii) *Εάν υποθέσουμε ότι δυο τυχόντα μη μηδενικά στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο και εάν θεωρήσουμε $a, b \in R \smallsetminus \{0_R\}$, τότε υπάρχει $d \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει*

$$d \in \text{ΜΚΔ}_R(a,b) \ \text{ και } \ td = ab, \ \text{όπου} \ \ t \in \text{ΕΚΠ}_R(a,b).$$

ΑΠΟΔΕΙΞΗ. (i) Εάν $a, b \in R \smallsetminus \{0_R\}$ και $d \in \text{ΜΚΔ}_R(a,b)$, τότε σύμφωνα με το λήμμα 5.2.28 υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε $a = da'$ και $b = db'$. Θέτοντας $t := da'b'$ παρατηρούμε ότι $t = ab' = ba'$. Εφαρμόζοντας τη συνεπαγωγή (ii)⇒(i) τού λήμματος 5.2.29 (με το στοιχείο a στη θέση τού εκεί παρατεθέντος b και το στοιχείο b στη θέση τού εκεί παρατεθέντος a) διαπιστώνουμε ότι $t \in \text{ΕΚΠ}_R(b,a) = \text{ΕΚΠ}_R(a,b)$. Επιπροσθέτως, εξ ορισμού τού t έχουμε $td = ab$.

(ii) Εάν $a, b \in R \smallsetminus \{0_R\}$ και $t \in \text{ΕΚΠ}_R(a,b)$, τότε σύμφωνα με το λήμμα 5.2.29 υπάρχουν σχετικώς πρώτα στοιχεία $a', b' \in R \smallsetminus \{0_R\}$, τέτοια ώστε $t = aa' = bb'$. Επειδή $a \mid ab$ και $b \mid ab$, από τον ορισμό 5.2.20 τού ελαχίστου κοινού πολλαπλασίου έπεται ότι $t \mid ab$. Κατά συνέπειαν, $\exists d \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει $ab = td$, οπότε

$$\left.\begin{array}{r} ab = td = aa'd \\ ba = td = bb'd \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b = a'd = da' \\ a = b'd = db' \end{array}\right\},$$

καθότι ο θεωρηθείς δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή (βλ. 1.2.5). Επειδή τα a', b' είναι σχετικώς πρώτα, εφαρμόζοντας τη συνεπαγωγή (ii)⇒(i) τού λήμματος 5.2.28 διαπιστώνουμε ότι $d \in \text{ΜΚΔ}_R(a,b)$. □

5.2.31 Λήμμα. *Έστω R μια ακεραία περιοχή. Εάν δυο τυχόντα στοιχεία τής R διαθέτουν πάντοτε κάποιον μέγιστο κοινό διαιρέτη και $a_1, a_2, a_3 \in R$, τότε*

$$\text{ΜΚΔ}_R(a_1,a_2,a_3) = \text{ΜΚΔ}_R(d,a_3),\ \forall d \in \text{ΜΚΔ}_R(a_1,a_2). \tag{5.12}$$

(*Ως εκ τούτου,* $\text{ΜΚΔ}_R(a_1,a_2,a_3) \neq \varnothing$.)

Αποδειξη. Θεωρούμε τυχόντες μεγίστους κοινούς διαιρέτες $d \in \text{ΜΚΔ}_R(a_1,a_2)$, $d' \in \text{ΜΚΔ}_R(d,a_3)$, καθώς και τυχόν $c \in R$ με $c \mid a_j$ για κάθε $j \in \{1,2,3\}$. Προφανώς,

$$\left.\begin{array}{r} d' \mid d \ \text{ και } \ d \mid a_1,\ d \mid a_2 \Rightarrow d' \mid a_1 \ \text{ και } \ d' \mid a_2 \\ d' \mid a_3 \end{array}\right\} \Rightarrow d' \mid a_j, \forall j \in \{1,2,3\}. \tag{5.13}$$

Από τον ορισμό 5.2.9 (εφαρμοζόμενον τόσον για τον d όσον και για τον d') λαμβάνουμε

$$c \mid a_1 \ \text{ και } \ c \mid a_2 \Rightarrow \ c \mid d, \quad c \mid d \ \text{ και } \ c \mid a_3 \Rightarrow \ c \mid d'. \tag{5.14}$$

Από τις (5.13) και (5.14) συμπεραίνουμε ότι $d' \in \text{ΜΚΔ}_R(a_1,a_2,a_3)$. Επομένως,

$$\text{ΜΚΔ}_R(a_1,a_2,a_3) \neq \varnothing \ \text{ και } \ \text{ΜΚΔ}_R(d,a_3) \subseteq \text{ΜΚΔ}_R(a_1,a_2,a_3).$$

Έστω τώρα τυχών $d'' \in \text{ΜΚΔ}_R(a_1,a_2,a_3)$. Από τον ορισμό 5.2.9 γνωρίζουμε ότι ισχύουν οι σχέσεις διαιρετότητας

$$d'' \mid a_1 \ \text{ και } \ d'' \mid a_2 \Rightarrow \ d'' \mid d, \quad d'' \mid d \ \text{ και } \ d'' \mid a_3 \Rightarrow \ d'' \mid d',$$

από τη μια μεριά και οι σχέσεις διαιρετότητας

$$\left.\begin{array}{r} d' \mid d \text{ και } d \mid a_1,\ d \mid a_2 \Rightarrow d' \mid a_1 \text{ και } d' \mid a_2 \\ d' \mid a_3 \\ d'' \in \mathrm{MK}\Delta_R(a_1, a_2, a_3) \end{array}\right\} \Rightarrow d' \mid d'',$$

από την άλλη. Αυτό σημαίνει ότι $d' \underset{\text{συν.}}{\sim} d''$. Από την πρόταση 5.2.12 συνάγουμε ότι $d' \in \mathrm{MK}\Delta_R(a_1, a_2, a_3)$ και $d'' \in \mathrm{MK}\Delta_R(d, a_3)$, απ' όπου έπεται ότι η (5.12) είναι αληθής. □

5.2.32 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα ακόλουθα:*

(i) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη.*

(ii) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο.*

(iii) *Εάν δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, και τανάπαλιν.*

(iv) *Εάν οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, τότε και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, και τανάπαλιν.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $n \in \mathbb{N}$, $n \geq 3$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία τού R, τότε -εξ υποθέσεως- οιοδήποτε ζεύγος εξ αυτών διαθέτει κάποιον μέγιστο κοινό διαιρέτη. Θα αποδείξουμε ότι ο ισχυρισμός είναι αληθής μέσω μαθηματικής επαγωγής. Έστω $n = 3$ και έστω $d \in \mathrm{MK}\Delta_R(a_1, a_2)$. Εάν $d' \in \mathrm{MK}\Delta_R(d, a_3)$, τότε σύμφωνα με το λήμμα 5.2.31 έχουμε

$$d' \in \mathrm{MK}\Delta_R(a_1, a_2, a_3).$$

Εν συνεχεία, υποθέτουμε ότι $n \geq 4$ και ότι ο ισχυρισμός μας είναι αληθής για τα $a_1, \ldots, a_{n-1}$. Έστω $d \in \mathrm{MK}\Delta_R(a_1, \ldots, a_{n-1})$. Εξ υποθέσεως, $\exists d' \in \mathrm{MK}\Delta_R(d, a_n)$. Έστω $c \in R$ με $c \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$. Προφανώς,

$$\left.\begin{array}{r} d' \mid d \text{ και } d \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \\ \Rightarrow d \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \\ d' \mid a_n \end{array}\right\} \Rightarrow d' \mid a_j, \forall j \in \{1, \ldots, n\}. \tag{5.15}$$

Από τον ορισμό 5.2.9 (εφαρμοζόμενον τόσον για τον d όσον και για τον d') λαμβάνουμε

$$c \mid a_j,\ \forall j \in \{1, \ldots, n-1\} \Rightarrow\ c \mid d, \quad c \mid d \text{ και } c \mid a_n \Rightarrow\ c \mid d'. \tag{5.16}$$

Από τις (5.15) και (5.16) συμπεραίνουμε ότι $d' \in \text{ΜΚΔ}_R(a_1, \ldots, a_{n-1}, a_n)$. Επομένως,

$$\text{ΜΚΔ}_R(a_1, \ldots, a_n) \neq \varnothing \ \text{ και } \ \text{ΜΚΔ}_R(d, a_n) \subseteq \text{ΜΚΔ}_R(a_1, \ldots, a_n).$$

(Με επιχειρήματα ανάλογα εκείνων που χρησιμοποιήθησαν στο λήμμα 5.2.31, όπου $n = 3$, μπορεί κανείς να δείξει ότι $\text{ΜΚΔ}_R(d, a_n) = \text{ΜΚΔ}_R(a_1, \ldots, a_n)$, αλλά εδώ αρκεί μόνον η διασφάλιση τής υπάρξεως *τουλάχιστον ενός* μεγίστου κοινού διαιρέτη των $a_1, \ldots, a_n$).

(ii) Εάν $n \in \mathbb{N}$, $n \geq 3$, και εάν τα $a_1, a_2, \ldots, a_n$ είναι στοιχεία τού R, τότε -εξ υποθέσεως- οιοδήποτε ζεύγος εξ αυτών διαθέτει κάποιο ελάχιστο κοινό πολλαπλάσιο. Θα αποδείξουμε ότι ο ισχυρισμός είναι αληθής μέσω μαθηματικής επαγωγής. Έστω $n = 3$ και έστω $t \in \text{ΕΚΠ}_R(a_1, a_2)$. Τότε

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \Longrightarrow \langle t \rangle \cap \langle a_3 \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle$$

και επειδή τα t και a_3 διαθέτουν κάποιο ελάχιστο κοινό πολλαπλάσιο, ας το πούμε t', με $\langle t' \rangle = \langle t \rangle \cap \langle a_3 \rangle$ (βλ. 5.2.24 (i)⇒(ii)), έχουμε

$$\langle t' \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle .$$

Τούτο σημαίνει ότι το t' είναι κατ' ανάγκην ένα ελάχιστο κοινό πολλαπλάσιο των a_1, a_2, a_3 (λόγω τού 5.2.24 (ii)⇒(i)). Εν συνεχεία, υποθέτουμε ότι $n \geq 4$ και ότι ο ισχυρισμός μας είναι αληθής για τα $a_1, \ldots, a_{n-1}$. Εάν το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_{n-1}$, τότε

$$\langle t \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_{n-1} \rangle \Longrightarrow \langle t \rangle \cap \langle a_n \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \cdots \cap \langle a_n \rangle ,$$

και επειδή τα t και a_n διαθέτουν (εξ υποθέσεως) κάποιο ελάχιστο κοινό πολλαπλάσιο, ας το πούμε t', με $\langle t' \rangle = \langle t \rangle \cap \langle a_n \rangle$ (βλ. 5.2.24 (i)⇒(ii)), έχουμε

$$\langle t' \rangle = \langle a_1 \rangle \cap \langle a_2 \rangle \cap \langle a_3 \rangle \cap \cdots \cap \langle a_{n-1} \rangle \cap \langle a_n \rangle ,$$

κάτι που σημαίνει ότι το t' είναι κατ' ανάγκην ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \ldots, a_n$ (λόγω τού 5.2.24 (ii)⇒(i)).

(iii) Κατ' αρχάς, υποθέτοντας ότι δυο τυχόντα στοιχεία τής R διαθέτουν μέγιστο κοινό διαιρέτη, θα αποδείξουμε ότι $\text{ΕΚΠ}_R(a, b) \neq \varnothing$ για οιαδήποτε $a, b \in R$. Εάν τουλάχιστον ένα εκ των a, b είναι $= 0_R$, τότε έχουμε $\text{ΕΚΠ}_R(a, b) = \{0_R\} \neq \varnothing$ (βλ. πόρισμα 5.2.26). Εάν $a, b \in R \smallsetminus \{0_R\}$, τότε η ύπαρξη κάποιου μεγίστου κοινού διαιρέτη $d \in \text{ΜΚΔ}_R(a, b)$ συνεπιφέρει την ύπαρξη ενός $t \in \text{ΕΚΠ}_R(a, b)$ με $td = ab$ επί τη βάσει τής προτάσεως 5.2.30.

Εν συνεχεία, υποθέτοντας ότι δυο τυχόντα στοιχεία τής R διαθέτουν ελάχιστο κοινό πολλαπλάσιο, θα αποδείξουμε ότι $\text{ΜΚΔ}_R(a, b) \neq \varnothing$ για οιαδήποτε $a, b \in R$.

Εάν $a = 0_R$, τότε προφανώς $b \in \mathrm{MK\Delta}_R(0_R, b)$. Κατ' αναλογίαν, εάν $b = 0_R$, τότε $a \in \mathrm{MK\Delta}_R(a, 0_R)$. Εάν $a, b \in R\smallsetminus\{0_R\}$, τότε η ύπαρξη κάποιου ελαχίστου κοινού πολλαπλασίου $t \in \mathrm{EK\Pi}_R(a, b)$ συνεπιφέρει την ύπαρξη ενός $d \in \mathrm{MK\Delta}_R(a, b)$ με $td = ab$ επί τη βάσει τής προτάσεως 5.2.30.

(iv) Τούτο έπεται άμεσα από τα (i), (ii) και (iii). □

5.2.33 Ορισμός. Έστω R μια ακεραία περιοχή. Η R καλείται **περιοχή με μέγιστο κοινό διαιρέτη** ή, εν συντομία, **περιοχή με μ.κ.δ.** όταν $\mathrm{MK\Delta}_R(a, b) \neq \varnothing$ για οιαδήποτε στοιχεία $a, b \in R$. (Εάν η R είναι περιοχή με μ.κ.δ., τότε, βάσει τής προτάσεως 5.2.32, και οιαδήποτε πεπερασμένου πλήθους στοιχεία τής R διαθέτουν τόσο μέγιστο κοινό διαιρέτη όσο και ελάχιστο κοινό πολλαπλάσιο).

5.2.34 Παράδειγμα. Κάθε Π.Κ.Ι. είναι περιοχή με μ.κ.δ. (Βλ. πόρισμα 5.2.15 ή, εναλλακτικώς, το πόρισμα 5.6.8 σε συνδυασμό με το θεώρημα 5.6.11.)

5.2.35 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a, b, c \in R$, τότε ισχύουν τα ακόλουθα:*

(i) $a \in \mathrm{MK\Delta}_R(a, a)$,

(ii) $a \mid b \Longleftrightarrow a \in \mathrm{MK\Delta}_R(a, b)$,

(iii) $\mathrm{MK\Delta}_R(d, c) = \mathrm{MK\Delta}_R(a, d'), \forall d \in \mathrm{MK\Delta}_R(a, b)$ *και* $\forall d' \in \mathrm{MK\Delta}_R(b, c)$,

(iv) $\mathrm{MK\Delta}_R(ca, cb) = \{\, cd \mid d \in \mathrm{MK\Delta}_R(a, b)\}$,

(v) $\mathrm{MK\Delta}_R(ab, c) = \mathrm{MK\Delta}_R(db, c)$, *για οιονδήποτε* $d \in \mathrm{MK\Delta}_R(a, c)$.

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $a \mid a$ και για κάθε $c \in R$ με $c \mid a$ ικανοποιούνται οι συνθήκες τού ορισμού 5.2.9 για το a, οπότε $a \in \mathrm{MK\Delta}_R(a, a)$.

(ii) Υποθέτοντας ότι $a \mid b$, έχουμε $a \mid a$ και $a \mid b$, και για κάθε $c \in R$ με $c \mid a$ και $c \mid b$ ικανοποιούνται οι συνθήκες τού ορισμού 5.2.9 για το a, οπότε $a \in \mathrm{MK\Delta}_R(a, b)$. Το αντίστροφο είναι προφανές.

(iii) Θεωρούμε τυχόντες $d \in \mathrm{MK\Delta}_R(a, b)$, $d' \in \mathrm{MK\Delta}_R(b, c)$. Εάν $d'' \in \mathrm{MK\Delta}_R(d, c)$ και $d''' \in \mathrm{MK\Delta}_R(a, d')$, αρκεί να δειχθεί ότι[5] $d'' \underset{\text{συν.}}{\sim} d'''$, ήτοι ότι $d'' \mid d'''$ και $d''' \mid d''$. Εξ υποθέσεως, $d'' \mid d$ και $d'' \mid c$. Επειδή $d \mid a$ και $d \mid b$, έχουμε $d'' \mid a$, $d'' \mid b$ και $d'' \mid c$. Από την άλλη μεριά, επειδή $d' \in \mathrm{MK\Delta}_R(b, c)$, έχουμε

$$\left.\begin{array}{r} d'' \mid a \ \text{ και } \ d'' \mid d' \\ d''' \in \mathrm{MK\Delta}_R(a, d') \end{array}\right\} \Rightarrow d'' \mid d'''.$$

Η σχέση διαιρετότητας $d''' \mid d''$ αποδεικνύεται παρομοίως.

[5] Εάν $d'' \underset{\text{συν.}}{\sim} d'''$, τότε από την πρόταση 5.2.12 συνάγουμε ότι $d''' \in \mathrm{MK\Delta}_R(d, c)$ και $d'' \in \mathrm{MK\Delta}_R(a, d')$, οπότε $\mathrm{MK\Delta}_R(d, c) = \mathrm{MK\Delta}_R(a, d')$.

(iv) Εάν $d \in \text{ΜΚΔ}_R(a,b)$ και $d' \in \text{ΜΚΔ}_R(ca,cb)$, αρκεί να δειχθεί ότι $d' \underset{\text{συν.}}{\sim} cd$, ήτοι ότι $d' \mid cd$ και $cd \mid d'$. Εάν $c = 0_R$, τούτο είναι προφανές, διότι

$$\text{ΜΚΔ}_R(0_R, 0_R) = \{0_R\}.$$

Εάν $c \neq 0_R$, τότε από τις σχέσεις διαιρετότητας $d \mid a$ και $d \mid b$ έπονται άμεσα οι $cd \mid ca$ και $cd \mid cb$ (βλ. 5.2.3 (ii)), οπότε $cd \mid d'$. Εξάλλου,

$$\left.\begin{array}{r} cd \mid d' \Rightarrow \exists r \in R : d' = (cd)\, r \\ d' \mid ca \Rightarrow \exists s \in R : ca = d's \\ d' \mid cb \Rightarrow \exists t \in R : cb = d't \end{array}\right\} \Rightarrow ca = cdrs,\ cb = cdrt.$$

Επειδή ο θεωρηθείς δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή, έχουμε

$$\left.\begin{array}{r} a = drs \\ b = drt \end{array}\right\} \Rightarrow dr \mid a \ \text{ και } \ dr \mid b$$

(βλ. 1.2.5), οπότε

$$d \in \text{ΜΚΔ}_R(a,b) \Rightarrow dr \mid d \Rightarrow d' = c\,(dr) \mid cd.$$

(v) Έστω τυχών $d \in \text{ΜΚΔ}_R(a,c)$. Κατά το (iv), $db \in \text{ΜΚΔ}_R(ab,cb)$. Έστω τυχών $d' \in \text{ΜΚΔ}_R(ab,cb)$. Τότε $d \underset{\text{συν.}}{\sim} d'$, οπότε

$$\left.\begin{array}{r} \text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(d',c) \\ \text{(iii)} \Rightarrow \text{ΜΚΔ}_R(d',c) = \text{ΜΚΔ}_R(ab,d''), \\ \forall d'' \in \text{ΜΚΔ}_R(cb,c) \end{array}\right\} \Rightarrow \left\{\begin{array}{c} \text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(ab,d''), \\ \forall d'' \in \text{ΜΚΔ}_R(cb,c) \end{array}\right\}$$

Κατά το (ii), $c \in \text{ΜΚΔ}_R(cb,c)$. Επιλέγοντας λοιπόν ως d'' το c, λαμβάνουμε $\text{ΜΚΔ}_R(db,c) = \text{ΜΚΔ}_R(ab,c)$. □

Ανάλογες ιδιότητες που αφορούν στα σύνολα των ελαχίστων κοινών πολλαπλασίων περιλαμβάνονται στην ακόλουθη πρόταση:

5.2.36 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a, b, c \in R$, τότε ισχύουν τα ακόλουθα:*

(i) $a \in \text{ΕΚΠ}_R(a,a)$,

(ii) $a \mid b \Longleftrightarrow b \in \text{ΕΚΠ}_R(a,b)$,

(iii) $\text{ΕΚΠ}_R(t,c) = \text{ΕΚΠ}_R(a,t')$, $\forall t \in \text{ΕΚΠ}_R(a,b)$ *και* $\forall t' \in \text{ΕΚΠ}_R(b,c)$,

(iv) $\text{ΕΚΠ}_R(ca,cb) = \{\, ct \mid t \in \text{ΕΚΠ}_R(a,b)\}$,

(v) $\text{ΕΚΠ}_R(ab,c) = \text{ΕΚΠ}_R(tb,c)$, *για οιοδήποτε* $t \in \text{ΕΚΠ}_R(a,c)$.

Επιπροσθέτως, η πρόταση 5.2.19 εξακολουθεί να ισχύει και για περιοχές με μ.κ.δ.

5.2.37 Πρόταση. *Έστω R μια περιοχή με μ.κ.δ. Εάν $a, b, c \in R$, τότε ισχύουν τα εξής:*

(i) *Εάν $a \mid bc$ και τα a, b είναι σχετικώς πρώτα, τότε $a \mid c$.*

(ii) *Εάν $a \mid c$, $b \mid c$ και τα a, b είναι σχετικώς πρώτα, τότε $ab \mid c$.*

(iii) *Εάν $c \mid a$ και τα a, b είναι σχετικώς πρώτα, τότε και τα c και b είναι σχετικώς πρώτα.*

► **Παράδειγμα ακεραίας περιοχής που δεν είναι περιοχή με μ.κ.δ.** Για την εύρεση παραδειγμάτων ακεραίων περιοχών που δεν είναι περιοχές με μ.κ.δ. θα εργασθούμε εντός τής κλάσεως των τετραγωνικών αριθμητικών περιοχών $\mathbb{Z}[\sqrt{m}]$ για κατάλληλους ακεραίους m στερούμενους τετραγώνων (βλ. άσκηση **1-37**). Συγκεκριμένα, στην πρόταση 5.2.42 θα αποδείξουμε ότι η $\mathbb{Z}[\sqrt{-5}]$ δεν είναι περιοχή με μ.κ.δ. Εν συνεχεία (στην πρόταση 5.3.8) θα καταλήξουμε στο ίδιο συμπέρασμα για τετραγωνικές αριθμητικές περιοχές $\mathbb{Z}[\sqrt{m}]$ αντιστοιχιζόμενες σε *απείρου πλήθους* ακεραίους m. Προτάσσουμε τον ορισμό τής *αριθμητικής στάθμης* τού $\mathbb{Q}(\sqrt{m})$, καθώς και τις βασικές ιδιότητες αυτής (οι οποίες, όπως θα διαπιστώσουμε τόσο στην παρούσα όσον και στις επόμενες ενότητες, υπεισέρχονται κατά τρόπο ουσιαστικό σε πληθώρα λίαν χρήσιμων εφαρμογών).

5.2.38 Ορισμός. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω $\mathbb{Q}(\sqrt{m}) \subsetneqq \mathbb{C}$ το τετραγωνικό αριθμητικό σώμα το αντιστοιχιζόμενο σε αυτόν. Εάν $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x, y \in \mathbb{Q})$, τότε λέμε ο $\overline{z} := x - y\sqrt{m}$ είναι ο **συζυγής**[6] τού z. Ως **αριθμητική στάθμη** τού $\mathbb{Q}(\sqrt{m})$ ορίζουμε την απεικόνιση $\mathbf{N} : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}$ μέσω τού τύπου

$$\boxed{\mathbf{N}(z) := z\overline{z} = (x + y\sqrt{m})(x - y\sqrt{m}) = x^2 - my^2,}$$

για κάθε $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x, y \in \mathbb{Q})$.

5.2.39 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $z, w \in \mathbb{Q}(\sqrt{m})$, τότε η αριθμητική στάθμη $\mathbf{N}$ τού τετραγωνικού αριθμητικού σώματος $\mathbb{Q}(\sqrt{m})$ έχει τις εξής ιδιότητες:*

[6] Όταν $m \leq -1$, τότε ο $\overline{z}$ είναι ο συζυγής τού $z \in \mathbb{C}$ *υπό τη συνήθη έννοια*:

$$x =: \mathrm{Re}(z), y\sqrt{m} = si\sqrt{|m|} =: \mathrm{Im}(z) \text{ και } \overline{z} := \mathrm{Re}(z) - \mathrm{Im}(z).$$

Όταν $m \geq 2$, τότε $z \in \mathbb{R}$ και "κατ' αναλογίαν" ο $x =: \mathrm{Rat}(z) \in \mathbb{Q}$ μπορεί να εκληφθεί ως το *ρητό μέρος* τού z και ο $y\sqrt{m} =: \mathrm{Irr}(z) \in \mathbb{R} \smallsetminus \mathbb{Q}$ ως το *άρρητο μέρος* τού z, με τον $\overline{z} := \mathrm{Rat}(z) - \mathrm{Irr}(z)$ ως συζυγή του. Σημειωτέον ότι

$$\boxed{z + \overline{z} = \begin{cases} 2\mathrm{Rat}(z), & \text{όταν } m \geq 2, \\ 2\,\mathrm{Re}(z), & \text{όταν } m \leq -1, \end{cases}} \text{ και } \boxed{z - \overline{z} = \begin{cases} 2\mathrm{Irr}(z), & \text{όταν } m \geq 2, \\ 2\,\mathrm{Im}(z), & \text{όταν } m \leq -1. \end{cases}}$$

(i) $\mathbf{N}(z) = 0 \Longleftrightarrow z = 0$.

(ii) $\mathbf{N}(zw) = \mathbf{N}(z)\,\mathbf{N}(w)$ *και* $|\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)|$.

(iii) *Εάν* $z \mid w$, *τότε* $\mathbf{N}(z) \mid \mathbf{N}(w)$ *και* $|\mathbf{N}(z)| \mid |\mathbf{N}(w)|$.

(iv) $z \in \mathbb{Z}[\sqrt{m}] \Rightarrow \mathbf{N}(z) \in \mathbb{Z}$.

(v) $z \in \mathbb{Z}[\sqrt{m}],\, m < 0 \Rightarrow \mathbf{N}(z) \in \mathbb{N}_0$.

(vi) $z \in \mathbb{Z}[\sqrt{m}]^{\times} \Longleftrightarrow \mathbf{N}(z) \in \{\pm 1\}$.

(vii) *Εάν* $z, w \in \mathbb{Z}[\sqrt{m}]$ *και* $z \underset{\text{συν.}}{\sim} w$, *τότε* $|\mathbf{N}(z)| = |\mathbf{N}(w)|$.

ΑΠΟΔΕΙΞΗ. (i) Εάν $z = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ $(x, y \in \mathbb{Q})$ με $\mathbf{N}(z) = 0$, τότε $y = 0$, διότι υποθέτοντας ότι $y \neq 0$, καταλήγουμε σε αντίφαση:

$$x^2 - my^2 = 0 \Longrightarrow m = \left(\frac{x}{y}\right)^2 \Longrightarrow \sqrt{m} \in \mathbb{Q},$$

Επομένως, $y = 0 \Rightarrow \mathbf{N}(z) = x^2 = 0 \Rightarrow x = 0 \Rightarrow z = 0$. Το αντίστροφο είναι προφανές.

(ii) Εάν

$$z = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m}),\ w = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})\ \ (r, s, x, y \in \mathbb{Q}),$$

τότε $zw = (rx + msy) + (ry + sx)\sqrt{m}$, οπότε

$$\begin{aligned} \mathbf{N}(zw) &= (rx + msy)^2 - m(ry + sx)^2 \\ &= r^2x^2 + m^2s^2y^2 - mr^2y^2 - ms^2x^2 \\ &= \left(r^2 - ms^2\right)\left(x^2 - my^2\right) = \mathbf{N}(z)\,\mathbf{N}(w). \end{aligned}$$

Η ισότητα $|\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)|$ είναι προφανής.

(iii) Τούτο έπεται άμεσα από το (ii).

(iv) Εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$, τότε

$$a, b, m \in \mathbb{Z} \Longrightarrow \mathbf{N}(z) = a^2 - mb^2 \in \mathbb{Z}.$$

(v) Εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$ και $m < 0$, τότε

$$a^2 \geq 0,\ b^2 \geq 0,\ -m > 0 \Longrightarrow \mathbf{N}(z) = a^2 - mb^2 \in \mathbb{N}_0.$$

(vi) Εάν $z \in \mathbb{Z}[\sqrt{m}]^{\times}$, τότε από το (ii) έπεται ότι

$$\left.\begin{array}{r} 1 = \mathbf{N}(1) = \mathbf{N}\left(zz^{-1}\right) = \mathbf{N}(z)\,\mathbf{N}\left(z^{-1}\right) \\ \text{(iii)} \Longrightarrow \mathbf{N}(z) \in \mathbb{Z},\ \mathbf{N}\left(z^{-1}\right) \in \mathbb{Z} \end{array}\right\} \Longrightarrow \mathbf{N}(z) \in \{\pm 1\}.$$

Και αντιστρόφως· εάν $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$ με

$$\mathbf{N}(z) = a^2 - mb^2 \in \{\pm 1\},$$

τότε

$$z(\mathbf{N}(z)\,\overline{z}) = (a + b\sqrt{m})(\mathbf{N}(z)\left(a - b\sqrt{m}\right)) = \mathbf{N}(z)^2 = 1,$$

οπότε το z έχει το $\mathbf{N}(z)\,\overline{z}$ ως αντίστροφό του.

(vii) Εάν $z, w \in \mathbb{Z}[\sqrt{m}]$ και $z \underset{\text{συν.}}{\sim} w$, τότε $z = uw$ για κάποιο $u \in \mathbb{Z}[\sqrt{m}]^{\times}$ (βλ. πόρισμα 5.2.5). Από τα (ii) και (vi) έπεται ότι

$$\mathbf{N}(z) = \mathbf{N}(uw) = \mathbf{N}(u)\,\mathbf{N}(w) \in \{\pm\mathbf{N}(w)\},$$

οπότε $|\mathbf{N}(z)| = |\mathbf{N}(w)|$. □

5.2.40 Παρατήρηση. Ως γνωστόν, $\mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}])$ (βλ. άσκηση **3-47**). Εάν λοιπόν $z = \frac{u}{w} \in \mathbb{Q}(\sqrt{m})$, όπου $(u, w) \in \mathbb{Z}[\sqrt{m}] \times (\mathbb{Z}[\sqrt{m}] \smallsetminus \{0\})$, τότε λόγω των ιδιοτήτων 5.2.39 (i) και (ii) έχουμε

$$u = zw \Rightarrow \mathbf{N}(u) = \mathbf{N}(zw) = \mathbf{N}(z)\,\mathbf{N}(w) \Rightarrow \mathbf{N}(z) = \tfrac{\mathbf{N}(u)}{\mathbf{N}(w)}.$$

5.2.41 Σημείωση. (Περί τής ομάδας των αντιστρεψίμων στοιχείων.)
Με τη βοήθεια τής ιδιότητας 5.2.39 (vi) είναι δυνατός ο ακριβής προσδιορισμός τής ομάδας $\mathbb{Z}[\sqrt{m}]^{\times}$ των αντιστρεψίμων στοιχείων τής τετραγωνικής αριθμητικής περιοχής $\mathbb{Z}[\sqrt{m}]$. Ένα στοιχείο $z = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ $(a, b \in \mathbb{Z})$, ανήκει στην $\mathbb{Z}[\sqrt{m}]^{\times}$ εάν και μόνον εάν το διατεταγμένο ζεύγος (a, b) ανήκει στο σύνολο των $(x, y) \in \mathbb{Z}^2$ που ικανοποιούν είτε τη διοφαντική εξίσωση

$$\boxed{x^2 - my^2 = 1} \tag{5.17}$$

είτε τη διοφαντική εξίσωση

$$\boxed{x^2 - my^2 = -1.} \tag{5.18}$$

(Διοφαντικές εξισώσεις αυτού τού τύπου καλούνται **εξισώσεις τού Pell**.) Διακρίνουμε δύο περιπτώσεις:

(i) Εάν $m \leq -1$, τότε η (5.18) δεν διαθέτει καμία ακεραία λύση (αφού $x^2 - my^2 \geq 0$ για κάθε $(x, y) \in \mathbb{Z}^2$), ενώ οι μόνες ακέραιες λύσεις τής (5.17) είναι οι $(\pm 1, 0)$ όταν $m < -1$ (αφού $y \neq 0 \Rightarrow x^2 - my^2 > 1$) και οι $(\pm 1, 0), (0, \pm 1)$ όταν $m = -1$ (αφού έχουμε κατ' ανάγκην $xy = 0$). Επομένως,

$$\boxed{\mathbb{Z}[\sqrt{m}]^{\times} = \begin{cases} \{\pm 1\}, & \text{όταν } m < -1, \\ \{\pm 1, \pm i\}, & \text{όταν } m = -1. \end{cases}}$$

(ii) Εάν $m \geq 2$, τότε το σύνολο των ακεραίων λύσεων τής (5.17) είναι πάντοτε μη κενό, ενώ τής (5.18) είναι αλλότε κενό και άλλοτε μη κενό. Από τη Θεωρία Αριθμών είναι γνωστό[7] το πώς (μέσω τού αναπτύγματος τής τετραγωνικής ρίζας $\sqrt{m}$ σε συνεχές κλάσμα) προσδιορίζεται η λεγόμενη *θεμελιώδης λύση* (x_1, y_1) των (5.17)-(5.18), ήτοι εκείνο το διατεταγμένο ζεύγος ακεραίων που ανήκει στο

$$\left\{(x,y) \in \mathbb{Z}^2 \middle| \, x^2 - my^2 \in \{\pm 1\}\right\} \tag{5.19}$$

και διαθέτει την *ελάχιστη δυνατή τετμημένη* και *μη μηδενική τεταγμένη*. Επίσης, είναι γνωστό ότι το (5.19) ισούται με το σύνολο

$$\left\{\pm(x_k, y_k) \in \mathbb{Z}^2 \middle| \, x_k + y_k\sqrt{m} = (x_1 + y_1\sqrt{m})^k, \ k \in \mathbb{Z}\right\},$$

απ' όπου έπεται ότι

$$\boxed{\mathbb{Z}[\sqrt{m}]^\times = \left\{ \pm(x_1 + y_1\sqrt{m})^k \middle| \ k \in \mathbb{Z}\right\}.}$$

Επί παραδείγματι, όταν $m = 2$ η θεμελιώδης λύση από το (5.19) (που ικανοποιεί, εν προκειμένω, την (5.18)) είναι η $(1,1)$, οπότε

$$\boxed{\mathbb{Z}[\sqrt{2}]^\times = \left\{\pm(1+\sqrt{2})^k \ | \ k \in \mathbb{Z}\right\}.}$$

Όταν $m = 3$, η (5.18) δεν διαθέτει ακέραιες λύσεις και η θεμελιώδης λύση από το (5.19) (που ικανοποιεί την (5.17)) είναι η $(2,1)$, οπότε

$$\boxed{\mathbb{Z}[\sqrt{3}]^\times = \left\{\pm(2+\sqrt{3})^k \ | \ k \in \mathbb{Z}\right\}.}$$

5.2.42 Πρόταση. *Για την τετραγωνική αριθμητική περιοχή* $\mathbb{Z}[\sqrt{-5}]$ *ισχύουν τα εξής:*

(i) $\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-5}]}(6, 2\left(1+\sqrt{-5}\right)) = \varnothing$.

(ii) $\text{ΕΚΠ}_{\mathbb{Z}[\sqrt{-5}]}(2, 1+\sqrt{-5}) = \varnothing$.

(iii) *Η* $\mathbb{Z}[\sqrt{-5}]$ *δεν είναι περιοχή με μ.κ.δ.*

ΑΠΟΔΕΙΞΗ. (i) Ας υποθέσουμε ότι για τα στοιχεία $6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ και $2\left(1+\sqrt{-5}\right)$ διαθέτουν κάποιον μέγιστο κοινό διαιρέτη, ας τον πούμε d. Βάσει τής προτάσεως 5.1.3 και τού (iii) τής προτάσεως 5.2.39,

$$\left.\begin{array}{r} d \mid 6 \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(6) = 36 \\ d \mid 2\left(1+\sqrt{-5}\right) \Rightarrow \mathbf{N}(d) \mid \mathbf{N}(2\left(1+\sqrt{-5}\right)) = 24 \\ \text{μκδ}\,(24, 36) = 12 \ (\text{εντός τού } \mathbb{Z}) \end{array}\right\} \Longrightarrow \mathbf{N}(d) \mid 12. \tag{5.20}$$

[7] Βλ., π.χ., Δ. Πουλάκη: *Θεωρία Αριθμών*, εκδόσεις Ζήτη, Θεσσαλονίκη, 1997, κεφ. 8, εν. 6, σελ. 206-212, και κεφ. 9, εν. 4, σελ. 231-232.

Επειδή $d \neq 0 \Longrightarrow \mathbf{N}(d) \geq 1$ (βλ. 5.2.39 (i) και (v)), έχουμε

$$\left.\begin{array}{r} 2 \mid 6 \;\; (\text{εντός τής } \mathbb{Z}[\sqrt{-5}]) \\ 2 \mid 2(1+\sqrt{-5}) \;\; (\text{εντός τής } \mathbb{Z}[\sqrt{-5}]) \end{array}\right\} \Longrightarrow 2 \mid d \Longrightarrow 4 = \mathbf{N}(2) \mid \mathbf{N}(d),$$

και

$$\left.\begin{array}{r} 1+\sqrt{-5} \mid 6 \;\; (\text{εντός τής } \mathbb{Z}[\sqrt{-5}]) \\ 1+\sqrt{-5} \mid 2(1+\sqrt{-5}) \;\; (\text{εντός τής } \mathbb{Z}[\sqrt{-5}]) \end{array}\right\} \Longrightarrow 6 = \mathbf{N}(1+\sqrt{-5}) \mid \mathbf{N}(d),$$

έχουμε

$$\left.\begin{array}{r} 4 \mid \mathbf{N}(d) \\ 6 \mid \mathbf{N}(d) \\ \text{εκπ}\,(4,6) = 12 \; (\text{εντός τού } \mathbb{Z}) \end{array}\right\} \Longrightarrow 12 \mid \mathbf{N}(d) \tag{5.21}$$

(βλ. πρόταση 5.1.5), οπότε οι σχέσεις διαιρετότητας (5.20) και (5.21) μας πληροφορούν ότι $\mathbf{N}(d) = 12$. Επιπροσθέτως, επειδή

$$1+\sqrt{-5} \mid d \Longrightarrow \exists a, b \in \mathbb{Z} : d = (1+\sqrt{-5})(a+b\sqrt{-5}),$$

έχουμε

$$\left.\begin{array}{r} 12 = \mathbf{N}(d) = 6 \cdot \mathbf{N}\left(a+b\sqrt{-5}\right) \\ \mathbf{N}\left(a+b\sqrt{-5}\right) = a^2+5b^2 \geq 0 \end{array}\right\} \Longrightarrow a^2+5b^2 = 2.$$

Η περίπτωση να ισχύει $b \neq 0$ *αποκλείεται*, διότι τότε θα είχαμε $a^2+5b^2 \geq 5$. Άρα κατ' ανάγκην $b = 0$. Όμως και η εξίσωση $a^2 = 2$ *δεν* διαθέτει ακέραιες λύσεις. Ως εκ τούτου, $\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-5}]}(6, 2\left(1+\sqrt{-5}\right)) = \varnothing$.

(ii) Ας υποθέσουμε ότι τα στοιχεία 2 και $1+\sqrt{-5}$ διαθέτουν κάποιο ελάχιστο κοινό πολλαπλάσιο t. Βάσει τής προτάσεως 5.1.5 και τού (iii) τής προτάσεως 5.2.39,

$$\left.\begin{array}{r} 2 \mid t \Rightarrow \mathbf{N}(2) = 4 \mid \mathbf{N}(t) \\ 1+\sqrt{-5} \mid t \Rightarrow \mathbf{N}(1+\sqrt{-5}) = 6 \mid \mathbf{N}(t) \\ \text{εκπ}\,(4,6) = 12 \; (\text{εντός τού } \mathbb{Z}) \end{array}\right\} \Longrightarrow 12 \mid \mathbf{N}(t). \tag{5.22}$$

Επειδή $t \neq 0 \Longrightarrow \mathbf{N}(t) \geq 1$ (βλ. 5.2.39 (i) και (v)) και

$$t \mid 2(1+\sqrt{-5}) \;\; (\text{εντός τής } \mathbb{Z}[\sqrt{-5}]) \Longrightarrow \mathbf{N}(t) \mid 24, \tag{5.23}$$

οι σχέσεις διαιρετότητας (5.22) και (5.23) μας πληροφορούν ότι $\mathbf{N}(t) \in \{12, 24\}$. Εάν $t = x + y\sqrt{-5}$, $x, y \in \mathbb{Z}$, τότε

$$\text{είτε } \; x^2+5y^2 = 12 \; \text{ είτε } \; x^2+5y^2 = 24.$$

Στην πρώτη περίπτωση πρέπει να ισχύει: $|y| \leq 1$ (διότι για $|y| \geq 2$ έχουμε προφανώς $x^2 + 5y^2 \geq 20$), οπότε $y \in \{0, \pm 1\}$. Για $y = 0$, η εξίσωση $x^2 = 12$ *δεν* διαθέτει ακέραιες λύσεις. Αλλά και για $y = \pm 1$, η εξίσωση $x^2 = 7$ *δεν* διαθέτει ακέραιες λύσεις. Άρα η πρώτη περίπτωση *αποκλείεται*. Στη δεύτερη περίπτωση πρέπει να ισχύει: $|y| \leq 2$ (διότι για $|y| \geq 3$ έχουμε $x^2 + 5y^2 \geq 45$) και $|x| \leq 4$ (διότι για $|x| \geq 5$ έχουμε $x^2 + 5y^2 \geq 25$). Από τον πίνακα όλων των δυνατών τιμών $(x, y) \neq (0, 0)$:

$\lvert x\rvert$	$\lvert y\rvert$	x^2+5y^2	$\lvert x\rvert$	$\lvert y\rvert$	x^2+5y^2
0	1	5	2	2	$\boxed{24}$
0	2	20	3	0	9
1	0	1	3	1	14
1	1	6	3	2	29
1	2	21	4	0	16
2	0	4	4	1	21
2	1	9	4	2	36

διαπιστώνουμε ότι οι μόνες ακέραιες λύσεις τής $x^2 + 5y^2 = 24$ είναι οι $x = \pm 2$ και $y = \pm 2$. Επομένως,

$$t \in \{\pm 2(1 + \sqrt{-5}), \pm 2(1 - \sqrt{-5})\}.$$

Επειδή τώρα το στοιχείο $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ είναι κοινό πολλαπλάσιο των 2 και $1 + \sqrt{-5}$ (εντός τής $\mathbb{Z}[\sqrt{-5}]$), πρέπει $t \mid 6$, ήτοι να υπάρχουν $u, v \in \mathbb{Z}$ με

$$6 \in \left\{\pm 2(1 + \sqrt{-5})(u + v\sqrt{-5}), \pm 2(1 - \sqrt{-5})(u + v\sqrt{-5})\right\},$$

ή, ισοδυνάμως,

$$\pm 3 \in \left\{(u - 5v) + (u + v)\sqrt{-5}, (u + 5v) + (u - v)\sqrt{-5}\right\}$$

πράγμα αδύνατο, καθότι οι $\pm 3 = \mp 6v$ δεν επιδέχονται ακέραιες λύσεις. Άρα *και* η δεύτερη περίπτωση *αποκλείεται*. Ως εκ τούτου, $\text{ΕΚΠ}_{\mathbb{Z}[\sqrt{-5}]}(2, 1 + \sqrt{-5}) = \varnothing$.

(iii) Τούτο έπεται άμεσα από το (i) ή -εναλλακτικώς- από το (ii). $\square$

5.3 ΠΡΩΤΑ ΚΑΙ ΑΝΑΓΩΓΑ ΣΤΟΙΧΕΙΑ

5.3.1 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο $p \in R$ καλείται **πρώτο στοιχείο** τού R όταν $p \in R \setminus (R^\times \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[p \mid ab \Longrightarrow \text{είτε } p \mid a \text{ είτε } p \mid b].$$

5.3.2 Ορισμός. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο $q \in R$ καλείται **ανάγωγο στοιχείο** τού R όταν $q \in R \setminus (R^{\times} \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[q = ab \Longrightarrow \text{είτε } \ a \in R^{\times} \ \text{ είτε } \ b \in R^{\times}].$$

5.3.3 Παραδείγματα. (i) Στον δακτύλιο $\mathbb{Z}$ των ακεραίων αριθμών ένα στοιχείο είναι πρώτο εάν και μόνο εάν είναι ανάγωγο, ήτοι τής μορφής $\pm p$, όπου p κάποιος πρώτος αριθμός.

(ii) Στον δακτύλιο $\mathbb{Z}_6$ (που είναι Δ.Κ.Ι. αλλά όχι Π.Κ.Ι.) το στοιχείο $[2]_6$ είναι πρώτο. Πράγματι· τα μόνα γινόμενα στοιχείων τού $\mathbb{Z}_6$ τα οποία διαιρεί το $[2]_6$ είναι τα

$$[1]_6\,[2]_6\,,[1]_6\,[4]_6\,,[2]_6\,[3]_6\,,[2]_6\,[4]_6\,,[2]_6\,[5]_6\,,[3]_6\,[4]_6\,,[4]_6\,[5]_6\,.$$

Αρκεί λοιπόν να παρατηρήσουμε ότι το $[2]_6$ διαιρεί τουλάχιστον έναν εκ των παραγόντων αυτών των γινομένων. Από την άλλη μεριά, το $[2]_6$ *δεν είναι* ανάγωγο στοιχείο τού $\mathbb{Z}_6$, αφού

$$[2]_6 = [4]_6\,[2]_6\,, \quad [4]_6 \notin \mathbb{Z}_6^{\times}, \quad [2]_6 \notin \mathbb{Z}_6^{\times}\,(= \{[1]_6\,, [5]_6\}).$$

(iii) Στην υποπεριοχή $R = \left\{ \frac{a}{2^n} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$ τού σώματος των ρητών αριθμών (βλ. άσκηση **1-25**) το στοιχείο $6 = \frac{6}{2^0}$ είναι ανάγωγο. Πράγματι· εάν το 6 γράφεται ως γινόμενο $6 = \frac{a}{2^n}\frac{b}{2^m}$, όπου $a, b \in \mathbb{Z},\ n, m \in \mathbb{N}_0$, τότε

$$ab = 2^{n+m+1} \cdot 3, \text{ με } n + m + 1 \geq 1,$$

απ' όπου έπεται ότι $3 \mid ab \Longrightarrow$ είτε $3 \mid a$ είτε $3 \mid b$ (εντός τού $\mathbb{Z}$!). Εάν $3 \mid a$, τότε $a = 3r$ για κάποιον $r \in \mathbb{Z}$, οπότε

$$rb = 2^{n+m+1} \Longrightarrow b = 2^{\mu}, \text{ για κάποιον } \mu \in \mathbb{N}_0,\ \mu \leq n + m + 1.$$

Κατά συνέπειαν, $\frac{b}{2^m} = 2^{\mu-m} \in R^{\times} = \{2^{\nu} \mid \nu \in \mathbb{Z}\}$. Εάν $3 \mid b$, τότε -κατ' αναλογίαν- $\frac{a}{2^n} \in R^{\times}$.

(iv) Στον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων τού Gauss (που είναι ακεραία περιοχή) ένα στοιχείο είναι πρώτο εάν και μόνο εάν είναι ανάγωγο (πρβλ. 5.3.4 (iv)). Μάλιστα, το θεώρημα **??** περιγράφει λεπτομερώς τη μορφή όλων των αναγώγων στοιχείων τού $\mathbb{Z}[i]$. Από την άλλη μεριά, στην ακεραία περιοχή $\mathbb{Z}[\sqrt{-3}]$ υπάρχουν ανάγωγα στοιχεία (όπως, π.χ., το 2) που δεν είναι πρώτα (βλ. τα (i) και (ii) τής προτάσεως 5.3.8).

5.3.4 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα ακόλουθα:*

(i) *Ένα $p \in R \smallsetminus (R^{\times} \cup \{0_R\})$ είναι πρώτο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R.*

(ii) *Ένα $q \in R \smallsetminus (R^{\times} \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των γνησίων μη τετριμμένων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό).*

(iii) *Κάθε πρώτο στοιχείο τής R είναι ανάγωγο*[8].

(iv) *Εάν η R είναι Π.Κ.Ι., τότε ένα $p \in R \smallsetminus (R^{\times} \cup \{0_R\})$ είναι πρώτο στοιχείο τής R εάν και μόνον εάν είναι ανάγωγο στοιχείο τής R.*

(v) *Εάν το p είναι ένα πρώτο στοιχείο τής R και $p \underset{\text{συν.}}{\sim} p'$, για κάποιο $p' \in R$, τότε και το p' είναι ένα πρώτο στοιχείο τής R.*

(vi) *Εάν το q είναι ένα ανάγωγο στοιχείο τής R και $q \underset{\text{συν.}}{\sim} q'$, για κάποιο $q' \in R$, τότε και το q' είναι ένα ανάγωγο στοιχείο τής R.*

(vii) *Οι μόνοι διαιρέτες ενός αναγώγου στοιχείου q τής R είναι τα συντροφικά του στοιχεία και τα αντιστρέψιμα στοιχεία τής R, ήτοι οι «μη γνήσιοι» διαιρέτες τού q* (βλ. 5.2.8).

(viii) *Ένα $q \in R \smallsetminus (R^{\times} \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν δεν διαθέτει «γνήσιους» διαιρέτες.*

ΑΠΟΔΕΙΞΗ. (i) Έστω $p \in R \smallsetminus (R^{\times} \cup \{0_R\})$ ένα πρώτο στοιχείο τής R. Επειδή το p είναι μη μηδενικό και μη αντιστρέψιμο, έχουμε $\{0_R\} \subsetneqq \langle p \rangle \subsetneqq R$. Υποθέτοντας ότι $a, b \in R$ με $ab \in \langle p \rangle$, έχουμε $p \mid ab$, οπότε είτε $p \mid a$ είτε $p \mid b$, δηλαδή είτε $a \in \langle p \rangle$ είτε $b \in \langle p \rangle$. Άρα το $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R. Και αντιστρόφως· υποθέτοντας ότι το το $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R, το στοιχείο p που το παράγει είναι μη μηδενικό και μη αντιστρέψιμο (βλ. 2.1.6), και εάν $a, b \in R$ με $p \mid ab$, τότε

$$ab \in \langle p \rangle \Longrightarrow \text{είτε } a \in \langle p \rangle \text{ είτε } b \in \langle p \rangle \Longrightarrow \text{είτε } p \mid a \text{ είτε } p \mid b,$$

οπότε το p είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής R.

(ii) Έστω q ένα ανάγωγο στοιχείο τής R. Προφανώς, $\{0_R\} \subsetneqq \langle q \rangle \subsetneqq R$. Έστω $\langle a \rangle$ τυχόν μη τετριμμένο γνήσιο κύριο ιδεώδες τής R με $\langle q \rangle \subseteq \langle a \rangle$. Τότε $q = ar$ για κάποιο $r \in R$. Επομένως, είτε $a \in R^{\times}$ είτε $r \in R^{\times}$. Η πρώτη περίπτωση αποκλείεται (καθότι υπετέθη πως το $\langle a \rangle$ είναι *γνήσιο* ιδεώδες τής R). Άρα $r \in R^{\times}$, οπότε

$$q \underset{\text{συν.}}{\sim} a \Longleftrightarrow \langle q \rangle = \langle a \rangle \Longrightarrow \left\{ \begin{array}{c} \text{Το } \langle q \rangle \text{ είναι ένα μεγιστικό στοιχείο} \\ \text{τού συνόλου όλων των μη τετριμμένων} \\ \text{γνησίων κυρίων ιδεωδών τής } R. \end{array} \right\}.$$

[8] Όπως είδαμε στο παράδειγμα 5.3.3 (ii), τούτο δεν είναι πάντοτε αληθές για μεταθετικούς δακτυλίους R με μοναδιαίο στοιχείο οι οποίοι *δεν είναι* ακέραιες περιοχές!

Και αντιστρόφως· εάν υποθέσουμε ότι το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό), τότε $\{0_R\} \subsetneqq \langle q \rangle \subsetneqq R$, οπότε το q δεν είναι ούτε $= 0_R$ ούτε αντιστρέψιμο. Επιπροσθέτως, εάν $a, b \in R$ με $q = ab$, έχουμε

$$\langle q \rangle \subseteq \langle a \rangle \Longrightarrow \text{είτε } \ \langle q \rangle = \langle a \rangle \ \text{ είτε } \ \langle a \rangle = R.$$

Εάν ισχύει η ισότητα $\langle q \rangle = \langle a \rangle$, τότε $a = qc$ για κάποιο $c \in R$, οπότε

$$q = ab = qbc \underset{(\text{βλ. } 1.2.5)}{\Longrightarrow} bc = 1 \Longrightarrow b \in R^{\times}.$$

Εάν, από την άλλη μεριά, ισχύει η ισότητα $\langle a \rangle = R$, τότε $a \in R^{\times}$. Κατά συνέπειαν, το q είναι ένα ανάγωγο στοιχείο τής R.

(iii) Έστω p ένα πρώτο στοιχείο τής R. Εάν $a, b \in R$ με $p = ab$, έχουμε

$$\text{είτε } \ p \mid a \ \text{ είτε } \ p \mid b \Longrightarrow \text{είτε } \left\{ \begin{array}{c} a = pr \\ \text{για κάποιο } r \in R \end{array} \right\} \text{ είτε } \left\{ \begin{array}{c} b = ps \\ \text{για κάποιο } s \in R \end{array} \right\}.$$

Επομένως, είτε $rb = 1$ είτε $sa = 1$, δηλαδή είτε $b \in R^{\times}$ είτε $a \in R^{\times}$. Άρα το p είναι ένα ανάγωγο στοιχείο τής R.

(iv) Λόγω τού (iii), αρκεί να αποδειχθεί ότι κάθε ανάγωγο στοιχείο μιας Π.Κ.Ι. R είναι πρώτο. Εάν λοιπόν το q είναι ανάγωγο, τότε $\{0_R\} \subsetneqq \langle q \rangle \subsetneqq R$ και (κατά το (ii)) το $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό). Επειδή η ακεραία περιοχή R είναι Π.Κ.Ι., το $\langle q \rangle$ είναι κατ' ανάγκην μεγιστικό ιδεώδες τής R. Όμως κάθε μεγιστικό ιδεώδες τής R είναι πρώτο ιδεώδες (βλ. θεώρημα 2.5.22). Άρα το $\langle q \rangle$ είναι πρώτο ιδεώδες και (βάσει τού (i)) το q είναι πρώτο στοιχείο τής R.

(v) Εάν το p είναι ένα πρώτο στοιχείο τής R και $p \underset{\text{συν.}}{\sim} p'$, τότε $p' = up$ για κάποιο $u \in R^{\times}$. Υποθέτοντας ότι $a, b \in R$ με $p' \mid ab$, έχουμε

$$\left. \begin{array}{c} p \mid p' \\ p' \mid ab \end{array} \right\} \Longrightarrow p \mid ab \Longrightarrow \text{είτε } \ p \mid a \ \text{ είτε } \ p \mid b.$$

Ως εκ τούτου, είτε $a = pr = u^{-1}p'r$ για κάποιο $r \in R$ είτε $b = ps = u^{-1}p's$ για κάποιο $s \in R$, απ' όπου συμπεραίνουμε ότι είτε $p' \mid a$ είτε $p' \mid b$. Κατά συνέπειαν, *και* το p'είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής R.

(vi) Εάν το q είναι ένα ανάγωγο στοιχείο τής R και $q \underset{\text{συν.}}{\sim} q'$, τότε $q = uq'$ για κάποιο $u \in R^{\times}$. Υποθέτοντας ότι $a, b \in R$ με $q' = ab$, έχουμε

$$q = uab \Longrightarrow \text{είτε } \ ua \in R^{\times} \ \text{ είτε } \ b \in R^{\times} \Longrightarrow \text{είτε } \ a \in R^{\times} \ \text{ είτε } \ b \in R^{\times},$$

οπότε *και* το q' είναι ένα ανάγωγο στοιχείο τής ακεραίας περιοχής R.

(vii) Έστω τυχόν $a \in R$ που είναι διαιρέτης τού q. Τότε $\langle q \rangle \subseteq \langle a \rangle$. Επειδή (κατά το (ii)) το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό στοιχείο τού συνόλου όλων των μη τετριμμένων γνησίων κυρίων ιδεωδών τής R (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό), συνάγουμε ότι $\langle q \rangle = \langle a \rangle$. Τούτο σημαίνει ότι είτε τα q και a είναι συντροφικά (βλ. 5.2.4 (ii)) είτε $\langle q \rangle = \langle a \rangle = R$, οπότε το a είναι αντιστρέψιμο.

(viii) Εάν το $q \in R \smallsetminus (R^\times \cup \{0_R\})$ είναι ανάγωγο στοιχείο τής ακεραίας περιοχής R, τότε αυτό δεν διαθέτει γνήσιους διαιρέτες βάσει τού (vii). Εάν, αντιστρόφως, ένα στοιχείο $q \in R \smallsetminus (R^\times \cup \{0_R\})$ δεν διαθέτει γνήσιους διαιρέτες και υπάρχουν $a, b \in R$, τέτοια ώστε να ισχύει η ισότητα $q = ab$, τότε, επειδή $a \mid q$ και $b \mid q$, έχουμε

$$\left(\text{είτε } a \in R^\times \text{ είτε } q \underset{\text{συν.}}{\sim} a\right) \text{ και } \left(\text{είτε } b \in R^\times \text{ είτε } q \underset{\text{συν.}}{\sim} b\right).$$

Υποθέτοντας ότι $q \underset{\text{συν.}}{\sim} a$ και $q \underset{\text{συν.}}{\sim} b$, συμπεραίνουμε ότι

$$q^2 \underset{\text{συν.}}{\sim} ab = q \Longrightarrow \exists x \in R^\times : q^2 = qx.$$

(βλ. 5.2.5 και 5.2.7). Επειδή ο θεωρούμενος δακτύλιος R είναι εξ υποθέσεως ακεραία περιοχή (βλ. 1.2.5), η ως άνω ισότητα ισοδυναμεί με την $q = x \in R^\times$, κάτι το οποίο είναι άτοπο. Άρα είτε $a \in R^\times$ είτε $b \in R^\times$ και, ως εκ τούτου, το q είναι ανάγωγο στοιχείο τής R. □

5.3.5 Πόρισμα. *Έστω R μια Π.Κ.Ι. Τότε ισχύουν τα ακόλουθα:*

(i) *Το p είναι πρώτο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle p \rangle$ είναι ένα μη τετριμμένο πρώτο ιδεώδες τής R.*

(ii) *Το q είναι ανάγωγο στοιχείο τής R εάν και μόνον εάν το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστικό ιδεώδες τής R.*

(iii) *Ένα στοιχείο τής R είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

(iv) *Ένα μη τετριμμένο ιδεώδες τής R είναι πρώτο εάν και μόνον εάν είναι μεγιστικό.*

ΑΠΟΔΕΙΞΗ. Είναι προφανές ότι τα (i), (ii) και (iv) έπονται άμεσα από την προηγηθείσα πρόταση 5.3.4. (Το (iv) είχε αποδειχθεί και ανεξαρτήτως αυτής στην πρόταση 4.2.15). Εξάλλου, επειδή κάθε ιδεώδες τής R είναι κύριο, το (iii) έπεται από το ότι κάθε μεγιστικό ιδεώδες τής R είναι μεγιστικό στοιχείο τού συνόλου των γνησίων ιδεωδών της και το (ii) τής 5.3.4. □

5.3.6 Πρόταση. *Ένα στοιχείο μιας περιοχής R με μ.κ.δ. είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

ΑΠΟΔΕΙΞΗ. Λόγω τού (iii) τής προτάσεως 5.3.4 αρκεί να αποδείξουμε ότι κάθε ανάγωγο στοιχείο τής R είναι πρώτο. Έστω $q \in R \smallsetminus (R^\times \cup \{0_R\})$ τυχόν ανάγωγο στοιχείο τής R. Ας υποθέσουμε ότι υπάρχουν $a, b \in R$, τέτοια ώστε $q \mid ab$. Εάν $q \nmid a$ και $d \in \text{ΜΚΔ}_R(q, a)$, τότε, σύμφωνα με το (ii) τής προτάσεως 5.2.35, $d \underset{\text{συν.}}{\not\sim} q$. Ωστόσο, $d \mid q$, οπότε υπάρχει $q' \in R$, τέτοιο ώστε να ισχύει η ισότητα $q = dq'$. Επειδή το q είναι ανάγωγο στοιχείο, έχουμε κατ' ανάγκην είτε $d \in R^\times$ είτε $q' \in R^\times$. Όμως $d \underset{\text{συν.}}{\not\sim} q \Longrightarrow q' \notin R^\times$. Κατά συνέπειαν, $d \in R^\times \Longrightarrow d \underset{\text{συν.}}{\sim} 1_R$, οπότε τα q και a είναι σχετικώς πρώτα. Από το (i) τής προτάσεως 5.2.37 συμπεραίνουμε ότι $q \mid b$. (Παρομοίως αποδεικνύεται, ύστερα από εναλλαγή των ρόλων των a και b, ότι εάν $q \nmid b$, τότε $q \mid a$.) Άρα το q είναι όντως πρώτο στοιχείο τής R. □

5.3.7 Παράδειγμα. Όπως έχουμε δείξει στα εδάφια 4.2.13 και 5.2.42, η ακεραία περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι ούτε Π.Κ.Ι. ούτε καν περιοχή με μ.κ.δ. Εναλλακτικώς, αυτό το συμπέρασμα μπορεί (λόγω τής 5.3.6) να εξαχθεί και απευθείας παρατηρώντας οτι το 2 είναι ανάγωγο, χωρίς όμως να είναι και πρώτο στοιχείο της. Όπως μας δείχνει η επόμενη πρόταση, η ιδιότητα αυτή ισχύει γενικότερα και για τετραγωνικές αριθμητικές περιοχές αντιστοιχιζόμενες σε *απείρου πλήθους* ακεραίους m.

5.3.8 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε ισχύουν τα ακόλουθα:*

(i) *Το 2 είναι δεν είναι πρώτο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$ (παρότι είναι πρώτο στοιχείο εντός τού $\mathbb{Z}$!)*

(ii) *Εάν για τον m ισχύει είτε $m \equiv 1 (\text{mod}\, 4)$ είτε $m \leq -3$, τότε το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$.*

(iii) *Εάν για τον m ισχύει είτε $m \equiv 1 (\text{mod}\, 4)$ είτε $m \leq -3$, τότε η $\mathbb{Z}[\sqrt{m}]$ δεν είναι ούτε Π.Κ.Ι. ούτε περιοχή με μκδ.*

ΑΠΟΔΕΙΞΗ. Επειδή $\mathbf{N}(2) = 4 \notin \{0, \pm 1\}$, έχουμε $2 \in \mathbb{Z}[\sqrt{m}] \smallsetminus (\mathbb{Z}[\sqrt{m}]^\times \cup \{0\})$ (επί τη βάσει των (i) και (vi) τής προτάσεως 5.2.39), όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$ (βλ. 5.2.38).

(i) Επειδή το γινόμενο $m(m-1) \in \mathbb{Z}$ είναι πάντοτε ένας άρτιος ακέραιος, έχουμε

$$2 \mid m(m-1) = \left(m + \sqrt{m}\right)\left(m - \sqrt{m}\right).$$

Εάν το 2 ήταν πρώτο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, θα έπρεπε

$$\text{είτε } \ 2 \mid m + \sqrt{m} \ \text{ είτε } \ 2 \mid m - \sqrt{m},$$

απ' όπου θα καταλήγαμε σε κάτι το οποίο είναι άτοπο, αφού εξισώσεις τής μορφής

$$m \pm \sqrt{m} = 2\left(x + y\sqrt{m}\right), \ x, y \in \mathbb{Z},$$

δεν επιδέχονται ακέραιες λύσεις ($2x = m$, $2y = \pm 1$). Άρα το 2 δεν είναι πρώτο στοιχείο τής ακεραίας περιοχής $\mathbb{Z}[\sqrt{m}]$.

(ii) Ας υποθέσουμε ότι το $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$, είναι ένας *γνήσιος* διαιρέτης τού 2 εντός τής $\mathbb{Z}[\sqrt{m}]$. Από τα (iii), (vi) και (vii) τής προτάσεως 5.2.39 έπεται ότι

$$\left.\begin{aligned} |\mathbf{N}\,(a+b\sqrt{m})| \mid |\mathbf{N}(2)| = 4 \\ \mathbf{N}\,(a+b\sqrt{m}) \neq \pm 1 \\ |\mathbf{N}\,(a+b\sqrt{m})| \neq |\mathbf{N}(2)| = 4 \end{aligned}\right\} \Longrightarrow \left|\mathbf{N}\left(a+b\sqrt{m}\right)\right| = 2,$$

οπότε

$$\pm\left(a^2 - mb^2\right) = 2. \tag{5.24}$$

Πρώτη περίπτωση. Εάν $m \equiv 1 (\operatorname{mod} 4)$, τότε $m = 4k + 1$ για κάποιον $k \in \mathbb{Z}$. Η ισότητα (5.24) γράφεται ως εξής:

$$a^2 - b^2 = 2\left(2kb^2 \pm 1\right). \tag{5.25}$$

Επειδή το δεξιό μέλος τής (5.25) είναι ένας άρτιος ακέραιος αριθμός, τα a και b οφείλουν να είναι *αμφότερα* είτε άρτιοι είτε περιττοί ακέραιοι. Εάν $a = 2\mu$ και $b = 2\nu$ για κάποιους $\mu, \nu \in \mathbb{Z}$, τότε

$$a^2 - b^2 = 4(\mu^2 - \nu^2) \Longrightarrow 4 \mid a^2 - b^2,$$

πράγμα αδύνατο (διότι $a^2 - b^2 \equiv 2(\operatorname{mod} 4)$ βάσει τής (5.25)). Εάν, από την άλλη μεριά, $a = 2u + 1$ και $b = 2v + 1$ για κάποιους $u, v \in \mathbb{Z}$, τότε και πάλι

$$a^2 - b^2 = 4(u^2 + u - v^2 - v) \Longrightarrow 4 \mid a^2 - b^2,$$

πράγμα που, όπως προείπαμε, είναι αδύνατο. Ως εκ τούτου, το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, αφού δεν διαθέτει γνήσιους διαιρέτες (βλ. το (viii) τής προτάσεως 5.3.4).

Δεύτερη περίπτωση. Εάν $m \leq -3$, τότε η ισότητα (5.24) γράφεται ως εξής:

$$2 = \left|a^2 - mb^2\right| = a^2 + |m|\, b^2. \tag{5.26}$$

Εάν $b = 0$, τότε η (5.26) είναι αδύνατη, αφού η $a^2 = 2$ δεν επιδέχεται ακέραιες λύσεις. Όμως η (5.26) είναι αναληθής ακόμη και όταν $b \neq 0$, επειδή

$$m \leq -3 \Longrightarrow |m| \geq 3 \Longrightarrow a^2 + |m|\, b^2 \geq 3.$$

Άρα το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$, αφού δεν διαθέτει γνήσιους διαιρέτες (βλ. το (viii) τής προτάσεως 5.3.4).

(iii) Τούτο έπεται άμεσα από τα (i), (ii), το (iv) τής προτάσεως 5.3.4 και την πρόταση 5.3.6. □

5.3.9 Πρόταση. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και έστω $z \in \mathbb{Z}[\sqrt{m}]$. Εάν $\mathbf{N}(z) \in \{\pm p\}$, όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$* (βλ. 5.2.38) *και p κάποιος πρώτος αριθμός, τότε το z είναι ανάγωγο στοιχείο τής τετραγωνικής αριθμητικής περιοχής $\mathbb{Z}[\sqrt{m}]$.*

ΑΠΟΔΕΙΞΗ. Επειδή $\mathbf{N}(z) \notin \{0, \pm 1\}$, έχουμε $z \in \mathbb{Z}[\sqrt{m}] \smallsetminus (\mathbb{Z}[\sqrt{m}]^{\times} \cup \{0\})$ (βλ. ιδιότητες 5.2.39 (i) και (vi)). Εάν τα u, w είναι στοιχεία τής $\mathbb{Z}[\sqrt{m}]$, τέτοια ώστε να ισχύει η ισότητα $z = uw$, τότε

$$\mathbf{N}(z) = \mathbf{N}(uw) = \mathbf{N}(u)\,\mathbf{N}(w) \in \{\pm p\}$$

οπότε *είτε* $\mathbf{N}(u) \in \{\pm 1\}$ και $\mathbf{N}(w) \in \{\pm p\}$ *είτε* $\mathbf{N}(w) \in \{\pm 1\}$ και $\mathbf{N}(u) \in \{\pm p\}$. Αυτό σημαίνει ότι είτε $u \in \mathbb{Z}[\sqrt{m}]^{\times}$ είτε $w \in \mathbb{Z}[\sqrt{m}]^{\times}$ (βλ. 5.2.39 (ii) και (vi)). Άρα το z είναι όντως ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{m}]$. □

5.3.10 Σημείωση. Η ικανή συνθήκη η οποία δίδεται στην πρόταση 5.3.9 προκειμένου ένα $z \in \mathbb{Z}[\sqrt{m}]$ να είναι ανάγωγο στοιχείο, δεν είναι και αναγκαία. Επί παραδείγματι, βάσει τής προτάσεως 5.3.8 το 2 είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{-3}]$ αλλά $\mathbf{N}(2) = 4$.

5.4 ΕΥΚΛΕΙΔΕΙΕΣ ΠΕΡΙΟΧΕΣ

5.4.1 Ορισμός. Έστω R μια ακεραία περιοχή. Η R ονομάζεται **ευκλείδεια περιοχή** όταν υπάρχει μια απεικόνιση $\boldsymbol{\delta} : R \smallsetminus \{0_R\} \longrightarrow \mathbb{N}_0$ που ικανοποιεί τις ακόλουθες συνθήκες:

(i) Εάν $a, b \in R \smallsetminus \{0_R\}$, τότε $\boldsymbol{\delta}(ab) \geq \boldsymbol{\delta}(a)$, και

(ii) για οιαδήποτε $a \in R$ και $b \in R \smallsetminus \{0_R\}$ υπάρχουν $(q, r) \in R \times R$ (όχι κατ' ανάγκην μονοσημάντως ορισμένα), τέτοια ώστε να ισχύει

$$\boxed{a = qb + r, \ \text{όπου είτε } r = 0_R \text{ είτε } (r \neq 0_R \text{ και } \boldsymbol{\delta}(r) < \boldsymbol{\delta}(b)).} \tag{5.27}$$

(Η απεινόνιση $\boldsymbol{\delta}$ καλείται **ευκλείδεια στάθμη** ή **ευκλείδεια εκτίμηση** τής R.)

5.4.2 Σημείωση. (i) Η συνθήκη (i) τού ορισμού 5.4.1 μπορεί να αναδιατυπωθεί ως εξής: Εάν $x, y \in R \smallsetminus \{0_R\}$ και $x \mid y$, τότε $\boldsymbol{\delta}(y) \geq \boldsymbol{\delta}(x)$.

(ii) Οι $(q, r) \in R \times R$ στην (5.27) καλούνται **πηλίκο** και, αντιστοίχως, **υπόλοιπο** τής **διαιρέσεως τού** a **διά τού** b **ως προς την** $\boldsymbol{\delta}$ *χωρίς*, ωστόσο, να χαίρουν κατ' ανάγκην *αμφοτέρων* των ιδιοτήτων των αντιστοίχων εννοιών που συναντήσαμε εργαζόμενοι στο σύνολο των ακεραίων αριθμών. (Βλ. εδάφιο 5.4.17, καθώς και την πρόταση 5.4.18, η οποία μας παρέχει μια ικανή και αναγκαία συνθήκη για τη διασφάλιση τής *μοναδικότητάς* τους, υπό τις προϋποθέσεις τού 5.4.1 (ii), *όχι* όμως και υπό την έννοια τού θεωρήματος 5.1.1!)

(iii) Μια ευκλείδεια περιοχή R εφοδιάζεται με απείρου πλήθους *διαφορετικές* ευκλείδειες στάθμες $\boldsymbol{\delta}$ (βλ. άσκηση ??). Ως εκ τούτου, όταν εργαζόμαστε με συγκεκριμένα παραδείγματα, η αναφορά μας σε κάποια ευκλείδεια περιοχή πρέπει να συνοδεύεται από τον τύπο ορισμού τής επιλεγόμενης $\boldsymbol{\delta}$.

5.4.3 Παραδείγματα. (i) Κάθε σώμα K καθίσταται ευκλείδεια περιοχή εφοδιαζόμενο με την ευκλείδεια στάθμη

$$\boldsymbol{\delta} : K\smallsetminus\{0_K\} \longrightarrow \mathbb{N}_0,\ \ \boldsymbol{\delta}(a) := 1,\ \forall a \in K\smallsetminus\{0_K\},$$

διότι για οιαδήποτε $a \in K$ και $b \in K\smallsetminus\{0_K\}$ ισχύει η (5.27) για τα $q = ab^{-1}$ και $r = 0_K$.

(ii) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων αριθμών είναι ευκλείδεια περιοχή όταν εφοδιάζεται με οιαδήποτε εκ των σταθμών

$$\boldsymbol{\delta}_k : \mathbb{Z}\smallsetminus\{0\} \longrightarrow \mathbb{N}_0,\ \ \boldsymbol{\delta}_k(a) := |a|^k,\ \forall a \in \mathbb{Z},\ \forall k \in \mathbb{N},$$

(βλ. άσκηση ??). Ειδικότερα, η $\boldsymbol{\delta}_1$ καλείται **συνήθης ευκλείδεια στάθμη** τού $\mathbb{Z}$.

(iii) Εάν επί τού υποσυνόλου των μη μηδενικών στοιχείων τού δακτυλίου

$$\mathbb{Z}_{\langle p\rangle} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; (a,b) \in \mathbb{Z}\times(\mathbb{Z}\smallsetminus\{0\}),\text{με μκδ}\,(a,b) = 1 \text{ και } p \nmid b \right\}$$

των p-αδικών κλασμάτων (όπου p πρώτος, βλ. άσκηση **1-11**, σελ. 34) ορίσουμε την απεικόνιση

$$\boldsymbol{\delta} : \mathbb{Z}_{\langle p\rangle}\smallsetminus\{0\} \longrightarrow \mathbb{N}_0,\ \ \boldsymbol{\delta}\left(\tfrac{a}{b}\right) := \max\left\{k \in \mathbb{N}_0 : p^k \mid a\right\},$$

(τη λεγομένη, ιδιαιτέρως, p-**αδική προσθετική εκτίμηση** τού $\mathbb{Z}_{\langle p\rangle}$), τότε, για οιαδήποτε στοιχεία $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{Z}_{\langle p\rangle}\smallsetminus\{0\}$, έχουμε προφανώς

$$\left.\begin{array}{r} \boldsymbol{\delta}\left(\frac{a_1}{b_1}\frac{a_2}{b_2}\right) = \boldsymbol{\delta}\left(\frac{a_1}{b_1}\right) + \boldsymbol{\delta}\left(\frac{a_2}{b_2}\right) \\ \boldsymbol{\delta}\left(\frac{a_2}{b_2}\right) \geq 0 \end{array}\right\} \Longrightarrow \boldsymbol{\delta}\left(\tfrac{a_1}{b_1}\tfrac{a_2}{b_2}\right) \geq \boldsymbol{\delta}\left(\tfrac{a_1}{b_1}\right).$$

Ας υποθέσουμε ότι $\frac{a_1}{b_1} \in \mathbb{Z}_{\langle p\rangle},\ \frac{a_2}{b_2} \in \mathbb{Z}_{\langle p\rangle}\smallsetminus\{0\}$ και ότι

$$\nu_1 := \max\left\{k \in \mathbb{N}_0 : p^k \mid a_1\right\},\ \ \nu_2 := \max\left\{k \in \mathbb{N}_0 : p^k \mid a_2\right\}.$$

Εάν διαιρέσουμε το a_1 διά τού a_2 (εντός τού $\mathbb{Z}$), λαμβάνουμε $a_1 = a_2\pi + \rho$, όπου το ζεύγος $(\pi, \rho) \in \mathbb{Z}$ είναι μονοσημάντως ορισμένο και ισχύει $0 \leq \rho \leq |a_2|$. Γράφοντας τα a_1 και a_2 ως $a_1 = p^{\nu_1}a_1', a_2 = p^{\nu_2}a_2'$, για κατάλληλα (μονοσημάντως ορισμένα) $a_1', a_2' \in \mathbb{Z}$ με μκδ$(a_1', p) =$ μκδ$(a_2', p) = 1$, ορίζουμε στοιχεία q και r τού $\mathbb{Z}_{\langle p \rangle}$ ως ακολούθως:

$$q := \begin{cases} \frac{a_1 b_2}{a_2 b_1}, & \text{όταν } \nu_1 \geq \nu_2, \\ \frac{\pi b_2}{b_1}, & \text{όταν } \nu_1 < \nu_2, \end{cases} \qquad r := \begin{cases} 0, & \text{όταν } \nu_1 \geq \nu_2, \\ \frac{\rho}{b_1}, & \text{όταν } \nu_1 < \nu_2. \end{cases}$$

Προφανώς, *και* στις δύο περιπτώσεις, ισχύει η ισότητα

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} q + r.$$

Όταν $\rho \neq 0$, τότε στη δεύτερη εξ αυτών (ήτοι όταν $\nu_1 < \nu_2$) έχουμε

$$\nu = \nu_1 < \nu_2 = \boldsymbol{\delta}\left(\tfrac{a_2}{b_2}\right),$$

όπου

$$\nu := \max\left\{k \in \mathbb{N}_0 : p^k \mid \rho\right\} = \boldsymbol{\delta}\left(\tfrac{\rho}{b_1}\right) = \boldsymbol{\delta}\left(r\right).$$

Πράγματι· επειδή

$$\rho = p^{\nu_1} a_1' - p^{\nu_2} a_2' \pi \Longrightarrow p^{\nu_1} \mid \rho,$$

συμπεραίνουμε ότι $\nu \geq \nu_1$. Υποθέτοντας ότι $\nu > \nu_1$, καταλήγουμε σε κάτι το άτοπο, καθόσον από τη σχέση διαιρετότητας $p^{\nu} \mid \rho$ έπεται ότι

$$p^{\nu_1} a_1' \equiv p^{\nu_2} a_2' \pi (\operatorname{mod} p^{\nu}) \quad \Longrightarrow \quad a_1' \equiv p^{\nu_2 - \nu_1} a_2' \pi (\operatorname{mod} p^{\nu - \nu_1})$$
$$\Downarrow$$
$$\exists \lambda \in \mathbb{Z} : a_1' = p(p^{\nu_2 - \nu_1 - 1} a_2' \pi + \lambda p^{\nu - \nu_1 - 1}),$$

ενώ $p \nmid a_1'$. Άρα όντως $\nu = \nu_1 < \nu_2$ και, βάσει των όσων προαναφέραμε, ο $\mathbb{Z}_{\langle p \rangle}$ καθίσταται ευκλείδεια περιοχή με την p-αδική προσθετική εκτίμηση ως ευκλείδεια στάθμη του.

(iv) Εκτός των (i)-(iii), στην κλάση των ευκλειδείων περιοχών συμπεριλαμβάνονται: ο δακτύλιος $K[\mathsf{X}]$ και ο δακτύλιος των επίτυπων δυναμοσειρών $K[\![\mathsf{X}]\!]$ (όπου K σώμα, βλ. προτάσεις 5.4.8 και 5.4.11), ορισμένες τετραγωνικές αριθμητικές περιοχές (βλ. πρόταση 5.4.16), καθώς και ορισμένοι εκ των δακτυλίων των ακεραίων των τετραγωνικών αριθμητικών σωμάτων. (Βλ. 5.5.7 και 5.5.8).

► **Διαίρεση πολυωνύμων και επίτυπων δυναμοσειρών**. Ο τρόπος εκτελέσεως τής «διαιρέσεως» ενός πολυωνύμου μιας απροσδιορίστου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ διά ενός πολυωνύμου $\psi(\mathsf{X}) \in K[\mathsf{X}] \smallsetminus \{0_{K[\mathsf{X}]}\}$ (όπου K σώμα) είναι γνωστός από το σχολείο και από τις παραδόσεις τής Εισαγωγικής Άλγεβρας. Άμεσες γενικεύσεις τής εν λόγω διαιρέσεως δίδονται στο θεώρημα 5.4.4 και στο πόρισμα 5.4.5.

5.4.4 Θεώρημα. (Γενικευμένος Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],\ \ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$$

με τους συντελεστές τους ειλημμένους από έναν μεταθετικό δακτύλιο R με μοναδιαίο στοιχείο, όπου $\mathrm{LC}(\psi(\mathsf{X})) = b_m$, υπάρχει ζεύγος πολυωνύμων $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$(\mathrm{LC}(\psi))^k \cdot \varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon(\mathsf{X}),\quad \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})) \tag{5.28}$$

ΑΠΟΔΕΙΞΗ. Εάν $\deg(\varphi(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε θέτοντας $k := 0$, $\varpi(\mathsf{X}) := 0_{R[\mathsf{X}]}$ και $\upsilon(\mathsf{X}) := \varphi(\mathsf{X})$, η (5.28) επαληθεύεται. Από εδώ λοιπόν και στο εξής μπορούμε να υποθέσουμε ότι

$$n = \deg(\varphi(\mathsf{X})) \geq \deg(\psi(\mathsf{X})) = m,\ \ n \geq 0.$$

Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον n. Εάν $n = 0$, τότε $m = 0$ και

$$\varphi(\mathsf{X}) = a_0,\ \ \psi(\mathsf{X}) = b_0,$$

οπότε αρκεί να θέσουμε $\varpi(\mathsf{X}) = a_0$, $\upsilon(\mathsf{X}) = 0_{R[\mathsf{X}]}$ και $k = 1$ για να λάβουμε την (5.28). Εν συνεχεία, υποθέτουμε ότι $n > 0$ και ότι *για κάθε πολυώνυμο* $\chi(\mathsf{X}) \in R[\mathsf{X}]$ *με* $\deg(\chi(\mathsf{X})) < n$ υπάρχει ένα ζεύγος πολυωνύμων $\varpi'(\mathsf{X})$ και $\upsilon'(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k' \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$(\mathrm{LC}(\psi(\mathsf{X})))^{k'} \chi(\mathsf{X}) = \varpi'(\mathsf{X})\psi(\mathsf{X}) + \upsilon'(\mathsf{X}),\quad \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})). \tag{5.29}$$

Ορίζουμε ως $\chi(\mathsf{X})$ το[9]

$$\chi(\mathsf{X}) := (\mathrm{LC}(\psi(\mathsf{X})))^k \varphi(\mathsf{X}) - a_n \mathsf{X}^{n-m} \psi(\mathsf{X}) \in R[\mathsf{X}].$$

Εάν $\chi(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε λαμβάνουμε εκ νέου την (5.28) θέτοντας

$$k := 1,\ \ \varpi(\mathsf{X}) := a_n \mathsf{X}^{n-m},\ \ \upsilon(\mathsf{X}) := 0_{R[\mathsf{X}]}.$$

Ειδάλλως, εκμεταλλευόμενοι την επαγωγική μας υπόθεση (5.29) θέτουμε

$$\upsilon(\mathsf{X}) := \upsilon'(\mathsf{X}),\ \ \varpi(\mathsf{X}) := \varpi'(\mathsf{X}) + (\mathrm{LC}(\psi(\mathsf{X})))^{k'} \left(a_n \mathsf{X}^{n-m}\right),\ \ k := k' + 1,$$

καταλήγοντας στην ισότητα

$$\begin{aligned} (\mathrm{LC}(\psi(\mathsf{X})))^k \varphi(\mathsf{X}) &= (\mathrm{LC}(\psi(\mathsf{X})))^{k'} \chi(\mathsf{X}) + (\mathrm{LC}(\psi(\mathsf{X})))^{k'} \left(a_n \mathsf{X}^{n-m} \psi(\mathsf{X})\right) \\ &= \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \end{aligned}$$

όπου $\deg(\upsilon(\mathsf{X})) = \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X}))$. □

[9] Ο συντελεστής τού προκειμένου $\chi(\mathsf{X})$ είναι ο $b_m a_n - a_n b_m = 0_R$, οπότε $\deg(\chi(\mathsf{X})) < n$.

5.4.5 Πόρισμα. (Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}], \ \ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\},$$

*με τους συντελεστές τους ειλημμένους από μια ακεραία περιοχή R, όπου $\mathrm{LC}(\psi(\mathsf{X})) = b_m \in R^{\times}$, υπάρχει ένα ζεύγος **μονοσημάντως ορισμένων** πολυωνύμων $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιων ώστε να ισχύει*

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon(\mathsf{X}), \ \ \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})). \tag{5.30}$$

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα 5.4.4 υπάρχει ένα ζεύγος πολυωνύμων $\varpi_*(\mathsf{X})$ και $\upsilon_*(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$(\mathrm{LC}(\psi(\mathsf{X})))^k \cdot \varphi(\mathsf{X}) = \varpi_*(\mathsf{X}) \cdot \psi(\mathsf{X}) + \upsilon_*(\mathsf{X}), \ \ \deg(\upsilon_*(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Επειδή $\mathrm{LC}(\psi) \in R^{\times}$ (οπότε και $(\mathrm{LC}(\psi))^k \in R^{\times}$), η (5.30) επαληθεύεται θέτοντας

$$\varpi(\mathsf{X}) := \varpi_*(\mathsf{X}) \left(\mathrm{LC}(\psi(\mathsf{X}))^k\right)^{-1}, \ \ \upsilon(\mathsf{X}) := \upsilon_*(\mathsf{X}) \left(\mathrm{LC}(\psi(\mathsf{X}))^k\right)^{-1}.$$

Αρκεί λοιπόν να αποδειχθεί και το *μονοσήμαντο* μιας τέτοιας εκφράσεως. Εάν πέραν των $\varpi(\mathsf{X})$, $\upsilon(\mathsf{X})$ υπάρχουν και άλλα δύο πολυώνυμα $\varpi'(\mathsf{X})$ και $\upsilon'(\mathsf{X})$, τα οποία πλήρουν τις[10]

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) = \varpi'(\mathsf{X})\psi(\mathsf{X}) + \upsilon'(\mathsf{X}),$$
$$\deg(\upsilon(\mathsf{X})) \leq \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})),$$

τότε

$$(\varpi(\mathsf{X}) - \varpi'(\mathsf{X}))\,\psi(\mathsf{X}) = \upsilon'(\mathsf{X}) - \upsilon(\mathsf{X}). \tag{5.31}$$

Υποθέτοντας ότι $\upsilon'(\mathsf{X}) \neq \upsilon(\mathsf{X})$, η (5.31) μας πληροφορεί ότι $\varpi(\mathsf{X}) \neq \varpi'(\mathsf{X})$, οπότε με τη βοήθεια τού (i) τού λήμματος 1.3.7 και τού (i) τής προτάσεως 1.3.9 συμπεραίνουμε ότι

$$\deg(\upsilon'(\mathsf{X})) \geq \deg(\upsilon'(\mathsf{X}) - \upsilon(\mathsf{X})) = \deg(\varpi(\mathsf{X}) - \varpi'(\mathsf{X})) + \deg(\psi(\mathsf{X})) \geq \deg(\psi(\mathsf{X})),$$

πράγμα που αντίκειται προς την ανίσωση $\deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X}))$. Συνεπώς,

$$\upsilon'(\mathsf{X}) = \upsilon(\mathsf{X}) \underset{(5.31)}{\Longrightarrow} (\varpi(\mathsf{X}) - \varpi'(\mathsf{X}))\,\psi(\mathsf{X}) = 0_{R[\mathsf{X}]} \Rightarrow \varpi(\mathsf{X}) = \varpi'(\mathsf{X}),$$

όπου η τελευταία συνεπαγωγή έπεται από το γεγονός ότι $\psi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$ και από το ότι ο δακτύλιος $R[\mathsf{X}]$ είναι μια ακεραία περιοχή (βλ. 1.3.9 (ii)). □

[10] Εάν $\deg(\upsilon'(\mathsf{X})) \leq \deg(\upsilon(\mathsf{X}))$, τότε επαναλαμβάνουμε τα ίδια αποδεικτικά επιχειρήματα εναλλάσσοντας τους ρόλους των $\upsilon(\mathsf{X})$ και $\upsilon'(\mathsf{X})$.

5.4.6 Ορισμός. Το πολυώνυμο $\varpi(\mathsf{X})$ στον τύπο (5.30) ονομάζεται **πηλίκο** και το $\upsilon(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\psi(\mathsf{X})$ εντός τού δακτυλίου $R\,[\mathsf{X}]$.

5.4.7 Παράδειγμα. Εάν

$$\varphi(\mathsf{X}) = \mathsf{X}^7 - 2\mathsf{X}^6 + \mathsf{X}^4 - \mathsf{X}^3 + 2\mathsf{X}^2 - 1, \quad \psi(\mathsf{X}) = \mathsf{X}^6 - 2\mathsf{X}^5 + 2\mathsf{X}^2 - 1 \in \mathbb{Z}[\mathsf{X}],$$

τότε

$$\varphi(\mathsf{X}) = \mathsf{X} \cdot \psi(\mathsf{X}) + \left(\mathsf{X}^4 - 3\mathsf{X}^3 + 2\mathsf{X}^2 + \mathsf{X} - 1\right).$$

5.4.8 Πρόταση. *Έστω K ένα σώμα. Τότε ο δακτύλιος των πολυωνύμων μιας απροσδιορίστου $K[\mathsf{X}]$ με συντελεστές ειλημμένους από το K καθίσταται ευκλείδεια περιοχή με την*

$$\boldsymbol{\delta} : K[\mathsf{X}] \smallsetminus \{0_{K[\mathsf{X}]}\} \longrightarrow \mathbb{N}_0, \;\; \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) := \deg(\varphi(\mathsf{X})), \tag{5.32}$$

ως ευκλείδεια στάθμη της.

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \smallsetminus \{0_{K[\mathsf{X}]}\}$, τότε σύμφωνα με το (i) τής προτάσεως 1.3.9 (ή το (i) τού πορίσματος 1.3.10) έχουμε

$$\begin{aligned} \boldsymbol{\delta}\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) &= \deg\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) \\ &= \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X})) \geq \deg\left(\varphi(\mathsf{X})\right) = \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right), \end{aligned}$$

οπότε η $\boldsymbol{\delta}$ ικανοποιεί τη συνθήκη 5.4.1 (i). Επιπροσθέτως, το πόρισμα 5.4.5 μας πληροφορεί ότι για οιαδήποτε πολυώνυμα $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ και $\psi(\mathsf{X}) \in K[\mathsf{X}] \smallsetminus \{0_{K[\mathsf{X}]}\}$ υπάρχουν $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi\,(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi\,(\mathsf{X})\right).$$

Εάν $\upsilon(\mathsf{X}) \neq 0_{K[\mathsf{X}]}$, τότε $\deg\left(\upsilon(\mathsf{X})\right) = \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) < \boldsymbol{\delta}\left(\psi(\mathsf{X})\right) = \deg\left(\psi\,(\mathsf{X})\right)$. Κατά συνέπειαν, η $\boldsymbol{\delta}$ ικανοποιεί *και* τη συνθήκη 5.4.1 (ii). □

5.4.9 Σημείωση. (i) Ευλόγως τίθεται το ερώτημα: Γιατί η πρόταση 5.4.8 δεν εξακολουθεί να ισχύει εάν κανείς αντικαταστήσει τον δακτύλιο $K[\mathsf{X}]$ με τον $R\,[\mathsf{X}]$, όπου R οιαδήποτε *ακεραία περιοχή* (αφού, μάλιστα, κατά την αποδεικτική διαδικασία χρησιμοποιήσαμε το (i) τής προτάσεως 1.3.9 και το πόρισμα 5.4.5 που ισχύουν για πολυώνυμα ανήκοντα στον $R\,[\mathsf{X}]$, όπου R τυχούσα *ακεραία περιοχή*); Για την απάντηση αυτού τού ερωτήματος οφείλουμε να ανατρέξουμε σε μια σημαντική λεπτομέρεια που περιλαμβάνεται στη διατύπωση τού πορίσματος 5.4.5. Εάν ο δακτύλιος αναφοράς μας R είναι μια ακεραία περιοχή που *δεν είναι* σώμα, τότε ορίζεται καλώς η (αντίστοιχη) απεικόνιση

$$\boldsymbol{\delta} : R\,[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\} \longrightarrow \mathbb{N}_0, \;\; \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}\left(\varphi(\mathsf{X})\right) := \deg(\varphi(\mathsf{X})),$$

η οποία ναι μεν ικανοποιεί τη συνθήκη 5.4.1 (i) αλλά δεν ικανοποιεί τη συνθήκη 5.4.1 (ii) για *όλα τα* $\psi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, παρά μόνον για όσα εξ αυτών έχουν επικεφαλής συντελεστή $\mathrm{LC}(\psi(\mathsf{X})) \in R^{\times} \subsetneqq R \smallsetminus \{0_R\}$. (Για κάθε σώμα K έχουμε $K^{\times} = K \smallsetminus \{0_K\}$!) Ως εκ τούτου, εντός τού $R[\mathsf{X}]$ μας επιτρέπεται να διαιρούμε τα πολυώνυμα $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ *μόνον* με εκείνα τα $\psi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$ που διαθέτουν αντιστρέψιμο επικεφαλής συντελεστή!

(ii) Γενικότερα ισχύει το εξής: Έστω R μια ακεραία περιοχή. Τότε ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι ευκλείδεια περιοχή *εάν και μόνον εάν* η R είναι σώμα. (Βλ. πρόταση 5.4.24.)

(iii) Η πρόταση 5.4.11 (η οποία μπορεί να εκληφθεί ως το ανάλογο τής προτάσεως 5.4.8 για επίτυπες δυναμοσειρές) μας πληροφορεί ότι ακόμη και ο δακτύλιος των επίτυπων δυναμοσειρών μιας απροσδιορίστου $K[\![\mathsf{X}]\!]$ με συντελεστές ειλημμένους από κάποιο σώμα K καθίσταται *κατά τρόπο φυσικό* ευκλείδεια περιοχή.

5.4.10 Πρόταση. (Αλγόριθμος Διαιρέσεως) *Δοθεισών δυο επίτυπων δυναμοσειρών*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!], \ \ \psi(\mathsf{X}) = \sum_{j=0}^{\infty} b_j \mathsf{X}^j \in K[\![\mathsf{X}]\!] \smallsetminus \{0_{K[\![\mathsf{X}]\!]}\},$$

με τους συντελεστές τους ειλημμένους από ένα σώμα K, υπάρχει ένα ζεύγος επίτυπων δυναμοσειρών $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\![\mathsf{X}]\!]$, τέτοιων ώστε να ισχύει [11]

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X}) \cdot \psi\,(\mathsf{X}) + \upsilon(\mathsf{X}), \tag{5.33}$$

όπου είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ *είτε* ($\upsilon(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ *και* $\mathrm{ord}(\upsilon(\mathsf{X})) < \mathrm{ord}(\psi\,(\mathsf{X}))$).

ΑΠΟΔΕΙΞΗ. Εάν ισχύει $\varphi(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ ή $\mathrm{ord}(\varphi(\mathsf{X})) < \mathrm{ord}(\psi(\mathsf{X}))$, τότε θέτοντας $\varpi(\mathsf{X}) := 0_{K[\![\mathsf{X}]\!]}$ και $\upsilon(\mathsf{X}) := \varphi(\mathsf{X})$, η (5.33) επαληθεύεται. Από εδώ λοιπόν και στο εξής μπορούμε να υποθέσουμε ότι $\varphi(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ και

$$n = \mathrm{ord}(\varphi(\mathsf{X})) \geq \mathrm{ord}(\psi(\mathsf{X})) = m.$$

Σύμφωνα με το (ii) τού πορίσματος 1.3.10 υπάρχουν (μονοσημάντως ορισμένες) επίτυπες δυναμοσειρές $\chi_1(\mathsf{X}), \chi_2(\mathsf{X}) \in K[\![\mathsf{X}]\!]^{\times}$, τέτοιες ώστε να ισχύουν οι ισότητες

$$\varphi(\mathsf{X}) = \mathsf{X}^n \chi_1(\mathsf{X}), \ \ \psi(\mathsf{X}) = \mathsf{X}^m \chi_2(\mathsf{X}).$$

[11] Σημειωτέον ότι, εν προκειμένω, όπως θα διαφανεί στην απόδειξη, είτε $\varpi(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$. Κατά συνέπειαν, για οιεσδήποτε επίτυπες δυναμοσειρές $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!] \smallsetminus \{0_{K[\![\mathsf{X}]\!]}\}$ έχουμε πάντοτε είτε $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})$ είτε $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$!

Θέτοντας $\varpi(\mathsf{X}) := \chi_1(\mathsf{X})\,(\chi_2(\mathsf{X}))^{-1}\,\mathsf{X}^{n-m}$ και $\upsilon(\mathsf{X}) := 0_{K[\![\mathsf{X}]\!]}$ λαμβάνουμε

$$\begin{aligned}\varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) &= \varpi(\mathsf{X})\psi(\mathsf{X}) \\ &= \left(\chi_1(\mathsf{X})\,(\chi_2(\mathsf{X}))^{-1}\,\mathsf{X}^{n-m}\right)\mathsf{X}^m\chi_2(\mathsf{X}) \\ &= \mathsf{X}^n\chi_1(\mathsf{X}) = \varphi(\mathsf{X}).\end{aligned}$$

οπότε η (5.33) επαληθεύεται και σε αυτήν την περίπτωση. □

5.4.11 Πρόταση. *Έστω K ένα σώμα. Τότε ο δακτύλιος των επίτυπων δυναμοσειρών μιας απροσδιορίστου $K[\![\mathsf{X}]\!]$ με συντελεστές ειλημμένους από το K καθίσταται ευκλείδεια περιοχή με την*

$$\boldsymbol{\delta} : K[\![\mathsf{X}]\!]\smallsetminus\{0_{K[\![\mathsf{X}]\!]}\} \longrightarrow \mathbb{N}_0,\;\; \varphi(\mathsf{X}) \mapsto \boldsymbol{\delta}(\varphi(\mathsf{X})) := \mathrm{ord}(\varphi(\mathsf{X})), \tag{5.34}$$

ως ευκλείδεια στάθμη της.

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\![\mathsf{X}]\!]\smallsetminus\{0_{K[\![\mathsf{X}]\!]}\}$, τότε σύμφωνα με το (ii) τού πορίσματος 1.3.10 έχουμε

$$\begin{aligned}\boldsymbol{\delta}(\varphi(\mathsf{X})\psi(\mathsf{X})) &= \mathrm{ord}(\varphi(\mathsf{X})\psi(\mathsf{X})) \\ &= \mathrm{ord}(\varphi(\mathsf{X})) + \mathrm{ord}(\psi(\mathsf{X})) \geq \mathrm{ord}(\varphi(\mathsf{X})) = \boldsymbol{\delta}(\varphi(\mathsf{X})),\end{aligned}$$

οπότε η $\boldsymbol{\delta}$ ικανοποιεί τη συνθήκη 5.4.1 (i). Επιπροσθέτως, η πρόταση 5.4.11 μας πληροφορεί ότι για οιεσδήποτε $\varphi(\mathsf{X}) \in K[\![\mathsf{X}]\!]$ και $\psi(\mathsf{X}) \in K[\![\mathsf{X}]\!]\smallsetminus\{0_{K[\![\mathsf{X}]\!]}\}$ υπάρχουν $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\![\mathsf{X}]\!]$, τέτοιες ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}),$$

όπου είτε $\upsilon(\mathsf{X}) = 0_{K[\![\mathsf{X}]\!]}$ είτε ($\upsilon(\mathsf{X}) \neq 0_{K[\![\mathsf{X}]\!]}$ και $\mathrm{ord}(\upsilon(\mathsf{X})) < \mathrm{ord}(\psi(\mathsf{X}))$). Κατά συνέπειαν, η $\boldsymbol{\delta}$ ικανοποιεί *και* τη συνθήκη 5.4.1 (ii). □

▶ **Κάποιες εκ των περιοχών $\mathbb{Z}[\sqrt{m}]$ είναι ευκλείδειες**. Φυσικό πρόβλημα: Για ποιους ακεραίους αριθμούς m στερουμένους τετραγώνων είναι η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ (η ορισθείσα στην άσκηση **1-37**) ευκλείδεια; Το πρόβλημα αυτό είναι δύσκολο, ορισμένες δε πτυχές του παραμένουν ακόμη και σήμερα ιδιαίτερα «σκοτεινές» (βλ. 5.5.9 (ii)). Στην πρόταση 5.4.16 αποδεικνύουμε ότι η $\mathbb{Z}[\sqrt{m}]$ είναι ευκλείδεια περιοχή όταν $m \in \{-2, -1, 2, 3, 6, 7\}$. Γενικεύσεις αυτής παρατίθενται στην ενότητα 5.5 (βλ. θεωρήματα 5.5.7 και 5.5.8).

5.4.12 Ορισμός. Έστω m ένας ακέραιος στερούμενος τετραγώνων. Τότε μια υποπεριοχή R τού τετραγωνικού αριθμητικού σώματος $\mathbb{Q}(\sqrt{m})$ καλείται **N-ευκλείδεια περιοχή** όταν αυτή καθίσταται ευκλείδεια περιοχή με στάθμη της την

$$\boldsymbol{\delta}_{\mathbf{N}} : R\smallsetminus\{0\} \longrightarrow \mathbb{N}_0,\;\; \boldsymbol{\delta}_{\mathbf{N}}(z) := |\mathbf{N}(z)| = |z\overline{z}|,\;\; \forall z \in R\smallsetminus\{0\}, \tag{5.35}$$

όπου $\mathbf{N}$ η αριθμητική στάθμη τού $\mathbb{Q}(\sqrt{m})$ (βλ. 5.2.38).

5.4.13 Παρατήρηση. Λόγω των ιδιοτήτων 5.2.39 (i) και (ii) τής $\mathbf{N}$ η συνθήκη 5.4.1 (i) ικανοποιείται από την $\boldsymbol{\delta}_{\mathbf{N}}$ για κάθε υποπεριοχή R τού $\mathbb{Q}(\sqrt{m})$. Πράγματι· για οιαδήποτε $z, w \in R\smallsetminus\{0\}$ έχουμε

$$\left.\begin{array}{r} |\mathbf{N}(zw)| = |\mathbf{N}(z)|\,|\mathbf{N}(w)| \\ w \neq 0 \Rightarrow |\mathbf{N}(w)| \geq 1 \end{array}\right\} \Longrightarrow \boldsymbol{\delta}_{\mathbf{N}}(zw) \geq \boldsymbol{\delta}_{\mathbf{N}}(z)\,.$$

Ως εκ τούτου, για να είναι μια τέτοια υποπεριοχή $\mathbf{N}$-ευκλείδεια αρκεί να προσδιορισθούν μόνον προϋποθέσεις υπό τις οποίες ικανοποιείται η συνθήκη 5.4.1 (ii). (Για την $R = \mathbb{Z}[\sqrt{m}]$ βλ. λήμμα 5.4.14.)

5.4.14 Λήμμα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν για οιαδήποτε $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}]\smallsetminus\{0\}$, το κλάσμα $\frac{z}{w}$, γραφόμενο υπό τη μορφή*

$$\frac{z}{w} = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}]), \;\; x, y \in \mathbb{Q}, \tag{5.36}$$

είναι τέτοιο, ώστε να υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη

$$\left|\mathbf{N}((a-x) + (b-y)\sqrt{m})\right| = \left|(a-x)^2 - m(b-y)^2\right| < 1, \tag{5.37}$$

τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή.

ΑΠΟΔΕΙΞΗ. Βάσει των προαναφερθέντων στο εδάφιο 5.4.13 αρκεί να αποδειχθεί ότι η $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii). Προς τούτο θεωρούμε τυχόντα στοιχεία $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}]\smallsetminus\{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w}$ υπό τη μορφή (5.59). Εξ υποθέσεως, υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη (5.37). Θέτοντας

$$q := a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}], \;\; r := z - qw \in \mathbb{Z}[\sqrt{m}],$$

παρατηρούμε ότι $z = qw + r$. Στην περίπτωση όπου $r \neq 0$ η (5.37) δίδει

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\mathbf{N}(\frac{z}{w} - q)\right| = \left|\mathbf{N}((a-x) + (b-y)\sqrt{m})\right| < 1,$$

οπότε (λόγω των προαναφερθέντων στο εδάφιο 5.2.40)

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\frac{\mathbf{N}(r)}{\mathbf{N}(w)}\right| = \frac{|\mathbf{N}(r)|}{|\mathbf{N}(w)|} = \frac{\boldsymbol{\delta}_{\mathbf{N}}(r)}{\boldsymbol{\delta}_{\mathbf{N}}(w)} < 1 \Rightarrow \boldsymbol{\delta}_{\mathbf{N}}(r) < \boldsymbol{\delta}_{\mathbf{N}}(w)\,.$$

Επομένως, η $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii) και η $\mathbb{Z}[\sqrt{m}]$ είναι $\mathbf{N}$-ευκλείδεια περιοχή. □

5.4.15 Λήμμα. *Εάν $\xi \in \mathbb{R}$, $0 \leq \xi < 2$ και $\xi \neq \frac{5}{4}$, τότε για κάθε $x \in \mathbb{R}$ υπάρχει κάποιος $a \in \mathbb{Z}$ για τον οποίο ισχύει*

$$\left|(a-x)^2 - \xi\right| < 1. \tag{5.38}$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε τον $\{x\}_{εγγ}$ (ήτοι τον ακέραιο το εγγύτερο τού x, βλ. 4.2.10), καθώς και τον $\breve{x} := \left|x - \{x\}_{εγγ}\right|$ με $0 \leq \breve{x} \leq \frac{1}{2}$, και θέτουμε

$$a' := \begin{cases} 0, & \text{όταν } 0 \leq \xi < 1, \\ 1, & \text{όταν } 1 \leq \xi < \frac{5}{4}, \\ -1, & \text{όταν } \frac{5}{4} < \xi < 2, \end{cases}$$

και

$$a := \begin{cases} a' - \{x\}_{εγγ}, & \text{όταν } x \geq \{x\}_{εγγ}, \\ -a' + \{x\}_{εγγ}, & \text{όταν } x < \{x\}_{εγγ}. \end{cases}$$

Προφανώς, $|a - x| = |\breve{x} - a'|$, οπότε

$$\left|(a-x)^2 - \xi\right| = \left|(\breve{x} - a')^2 - \xi\right|. \tag{5.39}$$

Εάν $0 \leq \xi < 1$, τότε $a' = 0$ και

$$\left.\begin{array}{r} 0 \leq \breve{x}^2 \leq \frac{1}{4} \\ -1 < -\xi \leq 0 \end{array}\right\} \Rightarrow -1 < \breve{x}^2 - \xi \leq \frac{1}{4} \Rightarrow \left|\breve{x}^2 - \xi\right| < 1. \tag{5.40}$$

Εάν $1 \leq \xi < \frac{5}{4}$, τότε $a' = 1$ και

$$\left.\begin{array}{r} \frac{1}{4} \leq (\breve{x}-1)^2 \leq 1 \\ -\frac{5}{4} < -\xi \leq -1 \end{array}\right\} \Rightarrow -1 < (\breve{x}-1)^2 - \xi \leq 0 \Rightarrow \left|(\breve{x}-1)^2 - \xi\right| < 1. \tag{5.41}$$

Εάν $\frac{5}{4} < \xi < 2$, τότε $a' = -1$ και

$$\left.\begin{array}{r} 1 \leq (\breve{x}+1)^2 \leq \frac{9}{4} \\ -2 < -\xi < -\frac{5}{4} \end{array}\right\} \Rightarrow -1 < (\breve{x}+1)^2 - \xi < 1 \Rightarrow \left|(\breve{x}+1)^2 - \xi\right| < 1. \tag{5.42}$$

Από τις (5.39), (5.40), (5.41) και (5.42) έπεται ότι η (5.38) είναι αληθής για τον ως άνω επιλεχθέντα ακέραιο a. $\square$

5.4.16 Πρόταση. *Εάν $m \in \{-2, -1, 2, 3, 6, 7\}$, τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$ είναι* **N**-*ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα στοιχεία $z \in \mathbb{Z}[\sqrt{m}]$ και $w \in \mathbb{Z}[\sqrt{m}] \smallsetminus \{0\}$, και γράφουμε το κλάσμα $\frac{z}{w}$ υπό τη μορφή

$$\frac{z}{w} = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m}) = \mathbf{Fr}(\mathbb{Z}[\sqrt{m}]), \quad x, y \in \mathbb{Q}. \tag{5.43}$$

Εν συνεχεία, θέτουμε $b := \{y\}_{εγγ}$ και διακρίνουμε δύο περιπτώσεις.

Περίπτωση πρώτη. Εάν $m \in \{-2,-1\}$, τότε θέτουμε $a := \{x\}_{\text{εγγ}}$ και παρατηρούμε ότι

$$\left.\begin{array}{l} |a-x| \leq \frac{1}{2} \\ |b-y| \leq \frac{1}{2} \end{array}\right\} \Rightarrow \left|(a-x)^2 - m(b-y)^2\right| \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1.$$

Επομένως, η συνθήκη (5.37) ικανοποιείται και η $\mathbb{Z}[\sqrt{m}]$ είναι **N**-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.4.14.

Περίπτωση δεύτερη. Εάν $m \in \{2,3,6,7\}$, τότε έχουμε

$$0 \leq m(b-y)^2 \leq \frac{7}{4} < 2 \;\text{ και }\; \sqrt{\tfrac{5m}{4}} \notin \mathbb{Q} \Rightarrow m(b-y)^2 \neq \frac{5}{4}.$$

Εφαρμόζοντας το λήμμα 5.4.15 για το $\xi := m(b-y)^2$ (και για το x το εμφανιζόμενο στην (5.43)) διασφαλίζουμε την ύπαρξη ενός $a \in \mathbb{Z}$ για τον οποίο ισχύει

$$\left|(a-x)^2 - m(b-y)^2\right| < 1.$$

Επομένως, η συνθήκη (5.37) ικανοποιείται και σε αυτήν την περίπτωση, και η $\mathbb{Z}[\sqrt{m}]$ είναι **N**-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.4.14. □

5.4.17 Παρατήρηση. Σύμφωνα με την πρόταση 5.4.16 ο δακτύλιος των γκαουσιανών ακεραίων $\mathbb{Z}[i]$ είναι **N**-ευκλείδεια περιοχή. Διαιρώντας τόν $3+2i$ διά τού $1+i$ εντός τού $\mathbb{Z}[i]$ ως προς την (5.35) έχουμε τη δυνατότητα να επιλέξουμε ως πηλίκο q και υπόλοιπο r *διαφορετικούς* μιγαδικούς αριθμούς ανήκοντες στον $\mathbb{Z}[i]$. Επί παραδείγματι,

$$\begin{aligned} 3+2i &= (1+i)\,(2-i)+i, \\ 3+2i &= (1+i)\,(3-i)-1, \\ 3+2i &= 2\,(1+i)+1, \\ 3+2i &= 3\,(1+i)-i, \end{aligned}$$

όπου *και* στις τέσσερεις περιπτώσεις $\boldsymbol{\delta}_{\mathbf{N}}(r) = 1 < 2 = \boldsymbol{\delta}_{\mathbf{N}}(1+i)$.

► **Γενικές ιδιότητες ευκλειδείων περιοχών**. Στα υπολειπόμενα εδάφια τής παρούσας ενότητας παρατίθενται ορισμένες γενικές ιδιότητες των ευκλειδείων περιοχών. Εξ αφορμής τής παρατηρήσεως 5.4.17 εκκινούμε από τη αποσαφήνιση τού πότε τα πηλίκα και τα υπόλοιπα τής διαιρέσεως στοιχείων μιας ευκλείδειας περιοχής R διά μη μηδενικών στοιχείων τής R (ως προς κάποια ευκλείδεια στάθμη $\boldsymbol{\delta}$) είναι *μονοσημάντως ορισμένα*.

5.4.18 Πρόταση. *Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R\smallsetminus\{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Τότε η ύπαρξη* μονοσημάντως ορισμένων $(q,r) \in R \times R$, *τα οποία ικανοποιούν την* (5.27) *για οιαδήποτε* $a \in R$ *και* $b \in R \smallsetminus \{0_R\}$, *ισοδυναμεί με τη συνθήκη*

$$\boldsymbol{\delta}(c-d) \leq \max\{\boldsymbol{\delta}(c), \boldsymbol{\delta}(d)\}, \ \forall (c,d) \in (R \smallsetminus \{0_R\}) \times (R \smallsetminus \{0_R\}) : c \neq -d. \quad (5.44)$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχουν μη μηδενικά, διακεκριμένα στοιχεία c, d τού R, τέτοια ώστε να ισχύει $\boldsymbol{\delta}(c-d) > \max\{\boldsymbol{\delta}(c), \boldsymbol{\delta}(d)\}$. Τότε

$$c = 0_R \cdot (c-d) + c, \quad \boldsymbol{\delta}(c) < \boldsymbol{\delta}(c-d),$$

και $c = 1 \cdot (c-d) + d, \quad \boldsymbol{\delta}(d) < \boldsymbol{\delta}(c-d)$, οπότε το πηλίκο και το υπόλοιπο τής διαιρέσεως τού $a := c$ διά τού $b := c-d$ δεν είναι μονοσημάντως ορισμένο.

Και αντιστρόφως· προϋποθέτοντας την ισχύ τής συνθήκης (5.44) και υποθέτοντας ότι

$$a = q_1 b + r_1, \ \text{ όπου είτε } \ r_1 = 0_R \ \text{ είτε } \ (r_1 \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r_1) < \boldsymbol{\delta}(b))$$

και

$$a = q_2 b + r_2, \ \text{ όπου είτε } \ r_2 = 0_R \ \text{ είτε } \ (r_2 \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r_2) < \boldsymbol{\delta}(b))$$

για κάποια $a \in R$ και $b \in R \smallsetminus \{0_R\}$ με $r_1 \neq r_2$ (και, κατ' επέκτασιν, $q_1 \neq q_2$), συνάγουμε (από την ιδιότητα (ii) τού ορισμού 5.4.1 για τα $q_1 - q_2$ και b, και την εφαρμογή τής συνθήκης (5.44) για τα $c := r_1$ και $d := r_2$) ότι

$$\boldsymbol{\delta}(b) \leq \boldsymbol{\delta}((q_1-q_2)\,b) = \boldsymbol{\delta}(r_1 - r_2) \leq \max\{\boldsymbol{\delta}(r_1), \boldsymbol{\delta}(r_2)\} < \boldsymbol{\delta}(b),$$

ήτοι κάτι το οποίο είναι άτοπο. Συνεπώς $r_1 = r_2$ και $(q_1 - q_2)\,b = 0_R \Longrightarrow q_1 = q_2$ (διότι $b \in R \smallsetminus \{0_R\}$, βλ. πρόταση 1.2.5). □

5.4.19 Παρατήρηση. (i) Εντός τού δακτυλίου $\mathbb{Z}[i]$ οι μιγαδικοί αριθμοί $c \in \{\pm 1\}$ και $d \in \{\pm i\}$ δεν πληρούν τη συνθήκη (5.44) ως προς την ευκλείδεια στάθμη (5.35), αφού

$$\boldsymbol{\delta}_{\mathbf{N}}(c-d) = 2 > \max\{\boldsymbol{\delta}_{\mathbf{N}}(c), \boldsymbol{\delta}_{\mathbf{N}}(d)\} = 1.$$

(ii) Παρότι η *συνήθης* ευκλείδεια στάθμη $\boldsymbol{\delta}(= \boldsymbol{\delta}_1) : \mathbb{Z} \smallsetminus \{0\} \longrightarrow \mathbb{N}_0$, $\boldsymbol{\delta}(a) := |a|$, τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών (βλ. 5.4.3 (ii)) *δεν* πληροί τη συνθήκη (5.44) για όλα τα ζεύγη μη μηδενικών μη αντιθέτων ακεραίων[12] (c, d), η *μοναδικότητα* τού πηλίκου q και τού υπολοίπου r τής διαιρέσεως ενός $a \in \mathbb{Z}$ διά ενός

[12]Π.χ., για $c = -7$ και $d = 2$ έχουμε $|c-d| = 9 > \max\{|c|, |d|\} = 7$, και για $a := c = -7$ και $b := c - d = -9$ λαμβάνουμε

$$-7 = 0 \cdot (-9) + (-7) = 1 \cdot (-9) + 2 \ \text{ με } \ |-7| < |-9|, \ |2| < |-9|.$$

$b \in \mathbb{Z} \smallsetminus \{0\}$ είναι διασφαλισμένη (στο πλαίσιο τής Στοιχειώδους Θεωρίας Αριθμών) *υπό τις επιπρόσθετες προϋποθέσεις* τού θεωρήματος 5.1.1, διότι σε αυτό αξιώσαμε *από το ίδιο* το εμφανιζόμενο υπόλοιπο r (και όχι μόνον από την απόλυτη τιμή του!) να είναι ≥ 0.

(iii) Έστω K ένα σώμα. Τότε η ευκλείδεια στάθμη (5.32) τού πολυωνυμικού δακτυλίου $K[\mathrm{X}]$ πληροί τη συνθήκη (5.44), οπότε η ιδιότητα τής *μοναδικότητας* των πηλίκων και των υπολοίπων η περιληφθείσα στο πόρισμα 5.4.5 έπεται (εναλλακτικώς) και από την πρόταση 5.4.18.

5.4.20 Πρόταση. *Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R \smallsetminus \{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Τότε ισχύουν τα ακόλουθα:*

(i) $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R)$, $\forall a \in R \smallsetminus \{0_R\}$.

(ii) *Εάν $a, b \in R \smallsetminus \{0_R\}$ και $a \underset{\text{συν.}}{\sim} b$, τότε $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(b)$.*

(iii) $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(-a)$, $\forall a \in R \smallsetminus \{0_R\}$.

(iv) $a \in R^{\times} \Longleftrightarrow a \in R \smallsetminus \{0_R\}$ *και* $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R)$.

ΑΠΟΔΕΙΞΗ. (i) Επειδή $a = a \cdot 1_R$, από την ιδιότητα (i) τού ορισμού 5.4.1 λαμβάνουμε $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R)$.

(ii) Εάν $a, b \in R \smallsetminus \{0_R\}$ και $a \underset{\text{συν.}}{\sim} b$, τότε $\exists x \in R^{\times} : a = bx$ (βλ. 5.2.5). Προφανώς, $b = ax^{-1}$, οπότε κάνοντας και πάλι χρήση τής ιδιότητας (i) τού ορισμού 5.4 .1 λαμβάνουμε

$$\left.\begin{array}{r} \boldsymbol{\delta}(a) = \boldsymbol{\delta}(bx) \geq \boldsymbol{\delta}(b) \\ \boldsymbol{\delta}(b) = \boldsymbol{\delta}\left(ax^{-1}\right) \geq \boldsymbol{\delta}(a) \end{array}\right\} \Longrightarrow \boldsymbol{\delta}(a) = \boldsymbol{\delta}(b).$$

(iii) Επειδή $-a = (-1_R)\, a$ και $a = (-1_R)(-a)$, έχουμε $a \underset{\text{συν.}}{\sim} -a$, οπότε αρκεί να εφαρμόσουμε το (ii).

(iv) Εάν $a \in R^{\times}$, τότε $a \in R \smallsetminus \{0_R\}$ και $\exists! a^{-1} \in R^{\times} : aa^{-1} = 1_R$, οπότε από το ανωτέρω (i) που έχουμε ήδη αποδείξει και την ιδιότητα (i) τού ορισμού 5.4.1 λαμβάνουμε

$$\left.\begin{array}{r} \boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(1_R) \\ \boldsymbol{\delta}(1_R) = \boldsymbol{\delta}\left(aa^{-1}\right) \geq \boldsymbol{\delta}(a) \end{array}\right\} \Longrightarrow \boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R).$$

Και αντιστρόφως· εάν $a \in R \smallsetminus \{0_R\}$ και $\boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R)$, τότε βάσει τής ιδιότητας (ii) τού ορισμού 5.4.1 υπάρχουν $(q, r) \in R \times R$, τέτοια ώστε να ισχύει

$$1_R = qa + r, \ \text{ όπου είτε } \ r = 0_R \ \text{ είτε } \ (r \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)).$$

Εάν υποθέσουμε ότι $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)$, τότε από την υπόθεσή μας και από το ανωτέρω (i) που έχουμε ήδη αποδείξει λαμβάνουμε

$$\boldsymbol{\delta}(1_R) \leq \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a) = \boldsymbol{\delta}(1_R),$$

ήτοι κάτι το οποίο είναι άτοπο. Ως εκ τούτου, $r = 0_R$ και $1_R = qa$, οπότε το a είναι αντιστρέψιμο. □

5.4.21 Θεώρημα. *Κάθε ευκλείδεια περιοχή είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R\smallsetminus\{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Το τετριμμένο ιδεώδες τής R είναι προφανώς κύριο. Αρκεί λοιπόν να αποδείξουμε ότι και κάθε μη τετριμμένο ιδεώδες τής R είναι κύριο. Υποθέτοντας ότι το I είναι τυχόν μη τετριμμένο ιδεώδες τής R, επιλέγουμε ένα $a \in I\smallsetminus\{0_R\}$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\delta}(a) = \min\{\,\boldsymbol{\delta}(x) \mid x \in I\smallsetminus\{0_R\}\}\,.$$

(Το σύνολο $\{\,\boldsymbol{\delta}(x) \mid x \in I\smallsetminus\{0_R\}\}$, όντας υποσύνολο τού $\mathbb{N}_0$, διαθέτει ελάχιστο στοιχείο.) Θα αποδείξουμε ότι $I = \langle a\rangle$. Προφανώς, $\langle a\rangle \subseteq I$. Εξάλλου, για οιοδήποτε $c \in I$, υπάρχουν $(q, r) \in R \times R$, τέτοια ώστε να ισχύει

$$c = qa + r, \ \text{ όπου είτε } \ r = 0_R \ \text{ είτε } \ (r \neq 0_R \ \text{ και } \ \boldsymbol{\delta}(r) < \boldsymbol{\delta}(a))\,.$$

Εάν λοιπόν υποθέσουμε ότι $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(a)$, τότε θα έχουμε

$$r = c - qa \in I \Longrightarrow \boldsymbol{\delta}(r) \in \{\,\boldsymbol{\delta}(x) \mid x \in I\smallsetminus\{0_R\}\} \Longrightarrow \boldsymbol{\delta}(r) \geq \boldsymbol{\delta}(a)\,,$$

ήτοι κάτι το οποίο είναι άτοπο. Ως εκ τούτου, $r = 0_R$ και $c = qa \in \langle a\rangle \Longrightarrow I \subseteq \langle a\rangle$, οπότε τελικώς $I = \langle a\rangle$. □

5.4.22 Παραδείγματα. Σύμφωνα με το θεώρημα 5.4.21, το (iii) τού εδαφίου 5.4.3 και τις προτάσεις 5.4.8, 5.4.11 και 5.4.16 οι δακτύλιοι

$$\mathbb{Z}_{\langle p\rangle}\ (p \text{ πρώτος}), \quad K[\mathsf{X}],\ K[\![\mathsf{X}]\!]\ (K \text{ σώμα}), \quad \mathbb{Z}[\sqrt{m}],\ m \in \{-2, -1, 2, 3, 6, 7\}\,,$$

είναι περιοχές κυρίων ιδεωδών.

5.4.23 Σημείωση. Για ορισμένες *ειδικές ακέραιες περιοχές* ισχύει και το αντίστροφο τού θεωρήματος 5.4.21 (βλ., π.χ., προτάσεις 5.4.24 και 5.4.26). Ωστόσο, αξίζει να επισημανθεί ότι η κλάση των ευκλειδείων περιοχών αποτελεί μια πολύ «ισχνή» υποκλάση τής κλάσεως των περιοχών κυρίων ιδεωδών! Παραδείγματα Π.Κ.Ι. που δεν είναι ευκλείδειες περιοχές δίδονται στην ενότητα 5.5.

5.4.24 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η ακεραία περιοχή $R[\mathsf{X}]$ είναι ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $R[\mathsf{X}]$ είναι Π.Κ.Ι.*

(iii) *Η ακεραία περιοχή R είναι σώμα.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο έπεται άμεσα από το θεώρημα 5.4.21.

(ii)⇒(iii) Ο επιμορφισμός δακτυλίων

$$R[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto a_0 \in R$$

έχει ως πυρήνα του το ιδεώδες $\langle \mathsf{X} \rangle$, οπότε το 1ο θεώρημα ισομορφισμών 3.3.3 μας πληροφορεί ότι $R[\mathsf{X}]/\langle \mathsf{X} \rangle \cong R$. Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, το $\langle \mathsf{X} \rangle$ είναι πρώτο ιδεώδες τού δακτυλίου $R[\mathsf{X}]$ (βλ. το (i) τού πορίσματος 3.1.10 και το θεώρημα 2.6.4). Επειδή ο $R[\mathsf{X}]$ είναι εξ υποθέσεως Π.Κ.Ι., το $\langle \mathsf{X} \rangle$ είναι μεγιστικό ιδεώδες του (βλ. την πρόταση 4.2.15 ή το (iv) τού πορίσματος 5.3.5), οπότε η R είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.10 και το πόρισμα 2.6.5).

(iii)⇒(i) Βλ. πρόταση 5.4.8. □

5.4.25 Πόρισμα. *Έστω K ένα σώμα και έστω R μια ακεραία περιοχή που δεν είναι σώμα. Τότε οι ακέραιες περιοχές $\mathbb{Z}[\mathsf{X}]$, $R[\mathsf{X}]$ και*

$$\mathbb{Z}[\mathsf{X}_1, \ldots, \mathsf{X}_n], \quad K[\mathsf{X}_1, \ldots, \mathsf{X}_n], \quad R[\mathsf{X}_1, \ldots, \mathsf{X}_n] \quad (n \geq 2)$$

δεν είναι ούτε ευκλείδειες περιοχές ούτε περιοχές κυρίων ιδεωδών.

5.4.26 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η ακεραία περιοχή $R[\![\mathsf{X}]\!]$ είναι ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $R[\![\mathsf{X}]\!]$ είναι Π.Κ.Ι.*

(iii) *Η ακεραία περιοχή R είναι σώμα.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο έπεται άμεσα από το θεώρημα 5.4.21.

(ii)⇒(iii) Ο επιμορφισμός δακτυλίων

$$R[\![\mathsf{X}]\!] \ni \sum_{i=0}^{\infty} a_i \mathsf{X}^i \longmapsto a_0 \in R$$

έχει ως πυρήνα του το ιδεώδες $\langle \mathsf{X} \rangle$, οπότε το 1ο θεώρημα ισομορφισμών 3.3.3 μας πληροφορεί ότι $R[\![\mathsf{X}]\!]/\langle \mathsf{X} \rangle \cong R$. Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως ακεραία περιοχή, το $\langle \mathsf{X} \rangle$ είναι πρώτο ιδεώδες τού δακτυλίου $R[\![\mathsf{X}]\!]$ (βλ. το (i) τού πορίσματος 3.1.10 και το θεώρημα 2.6.4). Επειδή ο $R[\![\mathsf{X}]\!]$ είναι εξ υποθέσεως Π.Κ.Ι., το $\langle \mathsf{X} \rangle$ είναι μεγιστικό ιδεώδες του (βλ. την πρόταση 4.2.15 ή το 5.3.5 (iv)), οπότε η ακεραία περιοχή R είναι σώμα (βλ. το (iii) τού πορίσματος 3.1.10 και το πόρισμα 2.6.5).

(iii)⇒(i) Βλ. πρόταση 5.4.11. □

5.4.27 Πόρισμα. *Έστω K ένα σώμα και έστω R μια ακεραία περιοχή που δεν είναι σώμα. Τότε οι ακέραιες περιοχές $\mathbb{Z}[\![\mathsf{X}]\!]$, $R[\![\mathsf{X}]\!]$ και*

$$\mathbb{Z}[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!], \quad K[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!], \quad R[\![\mathsf{X}_1, \ldots, \mathsf{X}_n]\!] \quad (n \geq 2)$$

δεν είναι ούτε ευκλείδειες περιοχές ούτε περιοχές κυρίων ιδεωδών.

► **Ευκλείδειος αλγόριθμος προσδιορισμού ενός μ.κ.δ.** Ο υπολογισμός *ενός* μεγίστου κοινού διαιρέτη τυχόντων μη μηδενικών στοιχείων $r_0 = a, r_1 = b$ μιας ευκλείδειας περιοχής R (ως προς μια δεδομένη ευκλείδεια στάθμη $\boldsymbol{\delta} : R \smallsetminus \{0_R\} \longrightarrow \mathbb{N}_0$) μπορεί να εκτελεσθεί με τη βοήθεια ενός αλγορίθμου, ο οποίος είναι ανάλογος τού *συνήθους* ευκλειδείου αλγορίθμου. Πράγματι· ας υποθέσουμε ότι $\boldsymbol{\delta}(a) \geq \boldsymbol{\delta}(b)$. Βάσει τής ιδιότητας (ii) τού ορισμού 5.4.1 υπάρχουν (όχι κατ' ανάγκην μονοσημάντως ορισμένα) ζεύγη στοιχείων (q_j, r_j), $1 \leq j \leq n+1$, $n \in \mathbb{N}_0$, τής R, ούτως ώστε να ισχύουν οι ισότητες:

$$\begin{cases} r_0 = q_1 r_1 + r_2, & \text{όπου είτε } r_2 = 0_R \text{ είτε } (r_2 \neq 0_R \text{ και } \boldsymbol{\delta}(r_2) < \boldsymbol{\delta}(r_1)), \\ r_1 = q_2 r_2 + r_3, & \text{όπου είτε } r_3 = 0_R \text{ είτε } (r_3 \neq 0_R \text{ και } \boldsymbol{\delta}(r_3) < \boldsymbol{\delta}(r_2)), \\ r_2 = q_3 r_3 + r_4, & \text{όπου είτε } r_4 = 0_R \text{ είτε } (r_4 \neq 0_R \text{ και } \boldsymbol{\delta}(r_4) < \boldsymbol{\delta}(r_3)), \\ \cdots\cdots & \cdots\cdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n, & \text{όπου είτε } r_n = 0_R \text{ είτε } (r_n \neq 0_R \text{ και } \boldsymbol{\delta}(r_n) < \boldsymbol{\delta}(r_{n-1})), \\ r_{n-1} = q_n r_n + r_{n+1}, & \text{όπου είτε } r_{n+1} = 0_R \text{ είτε } (r_{n+1} \neq 0_R \text{ και } \boldsymbol{\delta}(r_{n+1}) < \boldsymbol{\delta}(r_n)). \end{cases}$$

(*Σύμβαση*: Εάν $\exists r_j$, $j \geq 2$, με $r_j = 0_R$, τότε σταματούμε). Εξ αυτών συνάγουμε -ιδιαιτέρως- ότι

$$0 \leq \boldsymbol{\delta}(r_{n+1}) < \boldsymbol{\delta}(r_n) < \boldsymbol{\delta}(r_{n-1}) < \cdots < \boldsymbol{\delta}(r_3) < \boldsymbol{\delta}(r_2) < \boldsymbol{\delta}(r_1) \leq \boldsymbol{\delta}(r_0).$$

Εάν υποθέταμε ότι για *κάθε* φυσικό αριθμό n το r_{n+1} είναι $\neq 0_R$, θα καταλήγαμε στο συμπέρασμα ότι μεταξύ τού 0 και τού $\boldsymbol{\delta}(r_0)$ υπάρχουν *άπειροι* (σαφώς διακεκριμένοι) φυσικοί αριθμοί, κάτι που θα ήταν άτοπο. Ως εκ τούτου, υπάρχει (κατ' ανάγκην) κάποιος φυσικός αριθμός, ας τον πούμε n_*, για τον οποίο $r_{n_*} \neq 0_R$ και $r_{n_*+1} = 0_R$.

5.4.28 Πρόταση. (Ευκλείδειος αλγόριθμος) *Ο r_{n_*} είναι ένας μέγιστος κοινός διαιρέτης των a και b.*

ΑΠΟΔΕΙΞΗ. Εντός τού $\mathrm{Mat}_{2\times 2}(R)$ ισχύουν οι ισότητες

$$\begin{pmatrix} q_j & 1_R \\ 1_R & 0_R \end{pmatrix} \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \begin{pmatrix} r_{j-1} \\ r_j \end{pmatrix}, \ \forall j \in \{1, \ldots, n_*\}.$$

Θέτοντας

$$\mathbf{A} := \prod_{j=1}^{n_*} \begin{pmatrix} q_j & 1_R \\ 1_R & 0_R \end{pmatrix},$$

έχουμε

$$\mathbf{A}\begin{pmatrix} r_{n_*} \\ 0_R \end{pmatrix} = \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Από αυτήν την ισότητα έπεται ότι $a, b \in \langle r_{n_*} \rangle \Longrightarrow \langle a, b \rangle \subseteq \langle r_{n_*} \rangle$. Επιπροσθέτως, επειδή $\det(\mathbf{A}) = (-1_R)^{n_*} \in R^\times$, ο πίνακας $\mathbf{A}$ είναι αντιστρέψιμος (βλ. 1.2.13), οπότε

$$\begin{pmatrix} r_{n_*} \\ 0_R \end{pmatrix} = \mathbf{A}^{-1}\begin{pmatrix} a \\ b \end{pmatrix} \Longrightarrow r_{n_*} \in Ra + Rb = \langle a, b \rangle \Longrightarrow \langle r_{n_*} \rangle \subseteq \langle a, b \rangle .$$

Άρα $\langle r_{n_*} \rangle = \langle a, b \rangle$, πράγμα που σημαίνει ότι $r_{n_*} \in \mathrm{MK}\Delta_R(a, b)$ βάσει τού θεωρήματος 5.2.14. □

5.4.29 Παραδείγματα. (i) Εφαρμόζοντας τον ευκλείδειο αλγόριθμο 5.4.28 για τα στοιχεία $a = r_0 = 25 - 10i$ και $b = r_1 = 5 + i$ τού δακτυλίου $\mathbb{Z}[i]$ των ακεραίων τού Gauss (ως προς την ευκλείδεια στάθμη (5.35)) λαμβάνουμε

$$\begin{cases} 25 - 10i = (4 - 2i)(5 + i) + (3 - 4i), & \boldsymbol{\delta}_{\mathbf{N}}(3 - 4i) = 25 < 26 = \boldsymbol{\delta}_{\mathbf{N}}(5 + i), \\ 5 + i = (1 + i)(3 - 4i) + (-2 + 2i), & \boldsymbol{\delta}_{\mathbf{N}}(-2 + 2i) = 8 < 25 = \boldsymbol{\delta}_{\mathbf{N}}(3 - 4i), \\ 3 - 4i = (-1)(-2 + 2i) + (1 - 2i), & \boldsymbol{\delta}_{\mathbf{N}}(1 - 2i) = 5 < 8 = \boldsymbol{\delta}_{\mathbf{N}}(-2 + 2i), \\ -2 + 2i = (-1)(1 - 2i) - 1, & \boldsymbol{\delta}_{\mathbf{N}}(-1) = 1 < 5 = \boldsymbol{\delta}_{\mathbf{N}}(1 - 2i), \\ 1 - 2i = (-1 + 2i)(-1) + 0, & \end{cases}$$

απ' όπου συμπεραίνουμε ότι οι μιγαδικοί αριθμοί $25 - 10i$ και $5 + i$ είναι σχετικώς πρώτοι εντός τού $\mathbb{Z}[i]$.

(ii) Εφαρμόζοντας τον ευκλείδειο αλγόριθμο 5.4.28 για τα πολυώνυμα

$$\varphi(\mathsf{X}) = 2\mathsf{X}^4 + 5\mathsf{X}^3 - 5\mathsf{X} - 2 \in \mathbb{Q}[\mathsf{X}], \quad \psi(\mathsf{X}) = 2\mathsf{X}^3 - 3\mathsf{X}^2 - 2\mathsf{X} \in \mathbb{Q}[\mathsf{X}]$$

(ως προς την ευκλείδεια στάθμη (5.32)) λαμβάνουμε

$$\begin{cases} \varphi(\mathsf{X}) = (\mathsf{X} + 4)\,\psi(\mathsf{X}) + \left(14\mathsf{X}^2 + 3\mathsf{X} - 2\right), & \deg(4\mathsf{X}^2 + 3\mathsf{X} - 2) = 2 < 3, \\ \quad \psi(\mathsf{X}) = \left(\frac{1}{7}\mathsf{X} - \frac{12}{49}\right)\left(14\mathsf{X}^2 + 3\mathsf{X} - 2\right) & \\ \quad + \left(-\frac{48}{49}\mathsf{X} - \frac{24}{49}\right), & \deg(-\frac{48}{49}\mathsf{X} - \frac{24}{49}) = 1 < 2, \\ 14\mathsf{X}^2 + 3\mathsf{X} - 2 = \left(-\frac{343}{24}\mathsf{X} + \frac{49}{12}\right)\left(-\frac{48}{49}\mathsf{X} - \frac{24}{49}\right), & \end{cases}$$

απ' όπου συμπεραίνουμε ότι

$$-\frac{1}{49}(48\mathsf{X} + 24) \in \mathrm{MK}\Delta_{\mathbb{Q}[\mathsf{X}]}(\varphi(\mathsf{X}), \psi(\mathsf{X})).$$

Επειδή ο ευρεθείς μέγιστος κοινός διαιρέτης έχει περίπλοκους συντελεστές, είναι προτιμότερο να θεωρήσουμε αντ' αυτού το *μονοσημάντως ορισμένο* μονικό πολυώνυμο[13]

$$\left(-\frac{49}{48}\right)\left(-\frac{48}{49}\mathsf{X}-\frac{24}{49}\right)=\mathsf{X}+\frac{1}{2}\in \mathrm{MK}\Delta_{\mathbb{Q}[\mathsf{X}]}(\varphi(\mathsf{X}),\psi(\mathsf{X})).$$

5.5 ΠΕΡΙΟΧΕΣ ΚΥΡΙΩΝ ΙΔΕΩΔΩΝ ΟΙ ΟΠΟΙΕΣ ΔΕΝ ΕΙΝΑΙ ΕΥΚΛΕΙΔΕΙΕΣ ΠΕΡΙΟΧΕΣ

Για να εντοπίσουμε παραδείγματα περιοχών κυρίων ιδεωδών οι οποίες δεν είναι ευκλείδειες περιοχές θα εργασθούμε εντός τής οικογενείας *των δακτυλίων* $\mathfrak{O}_m$ *των ακεραίων των τετραγωνικών αριθμητικών σωμάτων* $\mathbb{Q}(\sqrt{m})$. Για $m<0$ ο δακτύλιος $\mathfrak{O}_m$ είναι Π.Κ.Ι. αλλά όχι και ευκλείδεια περιοχή εάν και μόνον εάν

$$m\in\{-163,-67,-43,-19\}$$

(βλ. πόρισμα 5.5.16).

5.5.1 Ορισμός. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Ο **δακτύλιος** $\mathfrak{O}_m$ **των ακεραίων** τού $\mathbb{Q}(\sqrt{m})$ είναι ο

$$\mathfrak{O}_m:=\left\{t\in\mathbb{Q}(\sqrt{m})\;\middle|\;t^2+ct+d=0,\;\;\text{για κάποια}\;\;c,d\in\mathbb{Z}\right\}.$$

(Είναι εύκολο να ελεγχθεί μέσω τής προτάσεως 5.5.2 ότι ο $\mathfrak{O}_m$ είναι ακεραία περιοχή, υποπεριοχή τού σώματος $\mathbb{C}$ όταν $m<0$ και υποπεριοχή τού σώματος $\mathbb{R}$ όταν $m>1$.)

5.5.2 Πρόταση. *Για οιονδήποτε ακέραιο αριθμό m στερούμενο τετραγώνων έχουμε*

$$\boxed{\mathfrak{O}_m=\begin{cases}\mathbb{Z}[\sqrt{m}], & \text{όταν}\; m\equiv 2(\mathrm{mod}\,4)\;\text{ή}\;\; m\equiv 3(\mathrm{mod}\,4),\\[2ex] \mathbb{Z}[\frac{1+\sqrt{m}}{2}], & \text{όταν}\; m\equiv 1(\mathrm{mod}\,4),\end{cases}}$$

όπου[14]

$$\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}]:=\left\{a+\tfrac{1+\sqrt{m}}{2}b\;\middle|\;a,b\in\mathbb{Z}\right\}=\left\{\tfrac{k+l\sqrt{m}}{2}\;\middle|\;k,l\in\mathbb{Z}\;\;\textit{και}\;\;k\equiv l(\mathrm{mod}\,2)\right\}.$$

---

[13] Πολλοί συγγραφείς ορίζουν «**τον**» *μέγιστο κοινό διαιρέτη* δύο πολυωνύμων $\varphi(\mathsf{X}),\psi(\mathsf{X})\in K[\mathsf{X}]$ (K σώμα) ως εκείνο το *μονοσημάντως ορισμένο* στοιχείο τού συνόλου $\mathrm{MK}\Delta_{K[\mathsf{X}]}(\varphi(\mathsf{X}),\psi(\mathsf{X}))$ που είναι μονικό πολυώνυμο. (Πρόκειται για το μονικό πολυώνυμο που είναι κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ και διαθέτει τον *μέγιστο δυνατό βαθμό*.)

[14] Όταν $m\equiv 1(\mathrm{mod}\,4)$, η ακεραία περιοχή $\mathbb{Z}[\sqrt{m}]$ περιέχεται *γνησίως* εντός τής $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

ΑΠΟΔΕΙΞΗ. "$\subseteq$": Έστω $t \in \mathbb{Q}(\sqrt{m})$ για το οποίο $t^2 + ct + d = 0$, για κάποια $c, d \in \mathbb{Z}$. Επειδή το t είναι τής μορφής $t = r + s\sqrt{m}$, όπου $r, s \in \mathbb{Q}$, έχουμε

$$\left(r + s\sqrt{m}\right)^2 + c\left(r + s\sqrt{m}\right) + d = 0 \Rightarrow \left(r^2 + s^2m + cr + d\right) + (2rs + cs)\sqrt{m} = 0,$$

απ' όπου έπεται ότι

$$r^2 + s^2m + cr + d = 0 \tag{5.45}$$

και

$$(2r + c)\, s = 0. \tag{5.46}$$

(i) Εάν $s = 0$, τότε $r \in \mathbb{Z}$. Πράγματι· γράφοντας το r ως *ανάγωγο* κλάσμα $r = \frac{a}{b}$, $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$, με μκδ$(a, b) = 1$, λαμβάνουμε μέσω τής (5.45):

$$\left.\begin{array}{r} cr + r^2 = -d \Longrightarrow cab + a^2 = -db^2 \\ \text{μκδ}\,(a, b) = 1 \end{array}\right\} \Longrightarrow a \mid d,$$

οπότε $cb + a = d'b^2$ για κάποιον $d' \in \mathbb{Z}$. Κατά συνέπειαν,

$$a = d'b^2 - cb \Longrightarrow b \mid a \Longrightarrow t = r \in \mathbb{Z}.$$

(ii) Υποθέτουμε ότι $s \neq 0$. Τότε η (5.46) δίδει

$$2r + c = 0 \Longrightarrow r = \frac{k}{2}, \text{ όπου } k := -c \in \mathbb{Z}, \tag{5.47}$$

και η (5.45) γράφεται ως

$$s^2m - r^2 + d = 0 \Longrightarrow s^2m - r^2 = -d \in \mathbb{Z}. \tag{5.48}$$

Γράφοντας, εν συνεχεία, το s ως *ανάγωγο* κλάσμα $s = \frac{p}{q}$, $(p, q) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$ με μκδ$(p, q) = 1$, λαμβάνουμε μέσω των (5.47) (5.48):

$$4p^2m - k^2q = -4q^2d \Longrightarrow 4p^2m = \left(k^2 - 4d\right) q^2,$$

οπότε

$$\left.\begin{array}{r} q^2 \mid 4p^2m \\ \text{μκδ}\,(p, q) = 1 \Longrightarrow \text{μκδ}\left(p^2, q^2\right) = 1 \end{array}\right\} \Longrightarrow q^2 \mid 4m.$$

Επειδή -εξ υποθέσεως- το m στερείται τετραγώνων, το q ισούται με ± 1 ή ± 2. Ως εκ τούτου, *και* στις δύο περιπτώσεις το s μπορεί να εκφρασθεί υπό τη μορφή

$$s = \tfrac{l}{2}, \text{ για κάποιον } l \in \mathbb{Z} \smallsetminus \{0\}. \tag{5.49}$$

Από τις (5.47), (5.48) και (5.49) έπεται ότι

$$\frac{l^2}{4}m - \frac{k^2}{4} \in \mathbb{Z} \Longleftrightarrow l^2 m - k^2 \equiv 0 (\bmod 4) \Longleftrightarrow l^2 m \equiv k^2 (\bmod 4). \tag{5.50}$$

Σημειωτέον ότι $m \not\equiv 0(\bmod 4)$, καθότι το m στερείται τετραγώνων. Οι υπόλοιπες περιπτώσεις θα εξετασθούν χωριστά.

Πρώτη περίπτωση: Εάν $m \equiv 1(\bmod 4)$, τότε $l^2 m \equiv l^2(\bmod 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv k^2(\bmod 4) \Longleftrightarrow (l-k)\,(l+k) \equiv 0(\bmod 4) \Longleftrightarrow k \equiv l(\bmod 2),$$

απ' όπου συμπεραίνουμε ότι $t \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

Δεύτερη περίπτωση: Εάν $m \equiv 2(\bmod 4)$, τότε $l^2 m \equiv 2l^2(\bmod 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv 2k^2(\bmod 4) \Leftrightarrow l^2 - 2k^2 \equiv 0(\bmod 4) \Leftrightarrow (k \equiv 0(\bmod 2) \text{ και } l \equiv 0(\bmod 2))\,,$$

απ' όπου συμπεραίνουμε ότι $t \in \mathbb{Z}[\sqrt{m}]$.

Τρίτη περίπτωση: Εάν $m \equiv 3(\bmod 4)$, τότε $l^2 m \equiv 3l^2(\bmod 4)$, οπότε η (5.50) καταλήγει στην ισοτιμία

$$l^2 \equiv 3k^2(\bmod 4) \Leftrightarrow l^2 - 3k^2 \equiv 0(\bmod 4) \Leftrightarrow (k \equiv 0(\bmod 2) \text{ και } l \equiv 0(\bmod 2))\,,$$

απ' όπου συμπεραίνουμε και πάλι ότι $t \in \mathbb{Z}[\sqrt{m}]$.

"$\supseteq$": Εάν $m \equiv 1(\bmod 4)$, και $t = \frac{k+l\sqrt{m}}{2} \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, όπου $k \equiv l(\bmod 2)$, τότε προφανώς

$$t^2 - kt + \tfrac{k^2 - l^2 m}{4} = 0,$$

όπου $k, \frac{k^2-l^2m}{4} \in \mathbb{Z}$, οπότε $t \in \mathfrak{O}_m$.

Εάν, από την άλλη μεριά, $m \equiv 2$ ή $3(\bmod 4)$ και $t = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, όπου $a, b \in \mathbb{Z}$, τότε

$$t^2 - at + a^2 - b^2 m = 0,$$

όπου a, $a^2 - b^2 m \in \mathbb{Z}$, οπότε και πάλι $t \in \mathfrak{O}_m$. □

5.5.3 Σημείωση. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων με $m \equiv 1(\bmod 4)$. Τότε ισχύουν τα εξής:

(i) Η τιμή τής αριθμητικής στάθμης οιουδήποτε στοιχείου

$$z = a + \tfrac{1+\sqrt{m}}{2}b = \left(a + \tfrac{b}{2}\right) + \tfrac{b}{2}\sqrt{m} \in \mathfrak{O}_m = \mathbb{Z}[\tfrac{1+\sqrt{m}}{2}]\;\; (a, b \in \mathbb{Z})$$

(βλ. 5.2.38) ισούται με

$$\boxed{\mathbf{N}(z)=\left(a+\tfrac{b}{2}\right)^2-\tfrac{mb^2}{4}=a^2+ab-\tfrac{(m-1)b^2}{4}\in\mathbb{Z}.}$$

Προφανώς, $\mathbf{N}(z)=0\Leftrightarrow z=0$ και

$$m<0\Longrightarrow \mathbf{N}(z)\geq 0. \tag{5.51}$$

(ii) Εάν $z\in\mathfrak{O}_m$, τότε $z\in\mathfrak{O}_m^\times \Longleftrightarrow \mathbf{N}(z)\in\{\pm1\}$. Πράγματι· εάν $z\in\mathfrak{O}_m^\times$, τότε

$$\left.\begin{array}{r} 1=\mathbf{N}(1)=\mathbf{N}\left(zz^{-1}\right)=\mathbf{N}(z)\,\mathbf{N}\left(z^{-1}\right) \\ \mathbf{N}(z)\in\mathbb{Z},\ \mathbf{N}\left(z^{-1}\right)\in\mathbb{Z} \end{array}\right\}\Rightarrow \mathbf{N}(z)\in\{\pm1\}.$$

Και αντιστρόφως· εάν $z=a+\frac{1+\sqrt{m}}{2}b\in\mathfrak{O}_m$ $(a,b\in\mathbb{Z})$ με $\mathbf{N}(z)\in\{\pm1\}$, τότε

$$z(\mathbf{N}(z)\,\overline{z})=\left(\left(a+\tfrac{b}{2}\right)+\tfrac{b}{2}\sqrt{m}\right)\left(\mathbf{N}(z)\left(\left(a+\tfrac{b}{2}\right)-\tfrac{b}{2}\sqrt{m}\right)\right)=\mathbf{N}(z)^2=1,$$

οπότε το z έχει το $\mathbf{N}(z)\,\overline{z}$ ως αντίστροφό του.

(iii) Μέσω τού (ii) είναι δυνατή η περιγραφή τής ομάδας $\mathfrak{O}_m^\times$ των αντιστρεψίμων στοιχείων τής $\mathfrak{O}_m$. Ένα στοιχείο

$$z=a+\tfrac{1+\sqrt{m}}{2}b=\left(a+\tfrac{b}{2}\right)+\tfrac{b}{2}\sqrt{m}\in\mathfrak{O}_m=\mathbb{Z}[\tfrac{1+\sqrt{m}}{2}]\ \ (a,b\in\mathbb{Z})$$

ανήκει στην $\mathfrak{O}_m^\times$ εάν και μόνον εάν το διατεταγμένο ζεύγος $(2a+b,b)$ ανήκει στο σύνολο των $(x,y)\in\mathbb{Z}^2$ που ικανοποιούν είτε τη διοφαντική εξίσωση

$$\boxed{x^2-my^2=4} \tag{5.52}$$

είτε τη διοφαντική εξίσωση

$$\boxed{x^2-my^2=-4.} \tag{5.53}$$

Ιδιαιτέρως, όταν $m\leq-3$ η (5.53) δεν διαθέτει καμία ακεραία λύση (αφού ισχύει $x^2-my^2\geq0$ για κάθε $(x,y)\in\mathbb{Z}^2$), ενώ οι μόνες ακέραιες λύσεις τής (5.52) είναι οι $(\pm2,0)$ για $m\leq-7$ (αφού $y\neq0\Rightarrow x^2-my^2>6$) και οι

$$(-2,0),(2,0),(1,1),(-1,1),(1,-1),(-1,-1)$$

για $m=-3$. Επομένως,

$$\boxed{m\equiv1(\operatorname{mod}4)\Rightarrow\mathfrak{O}_m^\times=\begin{cases}\{\pm1\}, & \text{όταν } m\leq-7,\\ \left\{\zeta_6^k\,|k\in\{0,1,2,3,4,5\}\right\}, & \text{όταν } m=-3,\end{cases}}$$

όπου $\zeta_6:=\exp(\frac{2\pi i}{6})$.

5.5.4 Λήμμα. *Έστω R μια ευκλείδεια περιοχή. Τότε $\exists u \in R\smallsetminus(R^{\times} \cup \{0_R\})$ με την εξής ιδιότητα: Για κάθε $z \in R$ υπάρχει ένα στοιχείο $r \in R^{\times} \cup \{0_R\}$ με $u \mid z - r$.*

ΑΠΟΔΕΙΞΗ. Έστω R μια ευκλείδεια περιοχή με την $\boldsymbol{\delta} : R\smallsetminus\{0_R\} \longrightarrow \mathbb{N}_0$ ως ευκλείδεια στάθμη της. Επιλέγουμε κάποιο στοιχείο $u \in R\smallsetminus(R^{\times} \cup \{0_R\})$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\delta}(u) = \min\left\{ \boldsymbol{\delta}(s) \mid s \in R\smallsetminus(R^{\times} \cup \{0_R\})\right\}.$$

Για κάθε $z \in R$ υπάρχουν $(q, r) \in R \times R$ με $z = uq + r$, όπου *είτε* $r = 0_R$ *είτε* $r \neq 0_R$ και $\boldsymbol{\delta}(r) < \boldsymbol{\delta}(u)$. Λόγω τού τρόπου επιλογής τού u έχουμε κατ' ανάγκην $r \in R^{\times} \cup \{0_R\}$. Επιπροσθέτως, είναι πρόδηλο ότι $u \mid z - r$. □

5.5.5 Λήμμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων. Εάν $m \leq -13$, τότε η ακεραία περιοχή $\mathfrak{O}_m$ δεν είναι ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι υπάρχει κάποιος ακέραιος $m \leq -13$ στερούμενος τετραγώνων, τέτοιος ώστε η $\mathfrak{O}_m$ να είναι ευκλείδεια περιοχή. Σημειωτέον ότι ισχύει $\mathfrak{O}_m^{\times} = \{\pm 1\}$ (βλ. 5.2.41 (i) όταν $m \not\equiv 1(\mathrm{mod}\, 4)$ και 5.5.3 (iii) όταν $m \equiv 1(\mathrm{mod}\, 4)$). Σύμφωνα με το λήμμα 5.5.4 υπάρχει κάποιο στοιχείο $u \in \mathfrak{O}_m\smallsetminus\{0, \pm 1\}$ με την εξής ιδιότητα: Για κάθε $z \in \mathfrak{O}_m$ $\exists r \in \{0, \pm 1\}$ με $u \mid z - r$. Αυτό σημαίνει ότι *για κάθε* $z \in \mathfrak{O}_m$ έχουμε

$$u \mid z \text{ ή } u \mid z - 1 \text{ ή } u \mid z + 1. \tag{5.54}$$

Εφαρμόζοντας τις συνθήκες διαιρετότητας (5.54) για την *ειδική* τιμή $z = 2$ λαμβάνουμε[15] $u \mid 2$ ή $u \mid 3$, οπότε

$$\exists v \in \mathfrak{O}_m : uv \in \{2, 3\}. \tag{5.55}$$

Επειδή $\mathbf{N}(2) = 4$ και $\mathbf{N}(3) = 9$, από το (5.55) έπεται ότι

$$\mathbf{N}(uv) \in \{4, 9\}. \tag{5.56}$$

Έστω ότι

$$u = \begin{cases} a + b\sqrt{m}, & \text{όταν } m \not\equiv 1(\mathrm{mod}\, 4), \\ a + \frac{1+\sqrt{m}}{2}b, & \text{όταν } m \equiv 1(\mathrm{mod}\, 4), \end{cases}$$

και

$$v = \begin{cases} a' + b'\sqrt{m}, & \text{όταν } m \not\equiv 1(\mathrm{mod}\, 4), \\ a' + \frac{1+\sqrt{m}}{2}b', & \text{όταν } m \equiv 1(\mathrm{mod}\, 4), \end{cases}$$

[15] Το ενδεχόμενο $u \mid 1$ αποκλείεται, διότι εξ υποθέσεως $u \notin \mathfrak{O}_m^{\times}$.

για κατάλληλους $a, b, a', b' \in \mathbb{Z}$. Εάν ίσχυε $u \in \mathfrak{O}_m \smallsetminus \mathbb{Z}$ (ήτοι $b \neq 0$) τότε θα είχαμε (λόγω τού (5.55)) $v \in \mathfrak{O}_m \smallsetminus \mathbb{Z}$ (ήτοι $b' \neq 0$) με

$$\mathbf{N}(u) = \begin{cases} a^2 - mb, & \text{όταν } m \not\equiv 1 (\operatorname{mod} 4), \\ \left(a + \frac{b}{2}\right)^2 - \frac{mb^2}{4}, & \text{όταν } m \equiv 1 (\operatorname{mod} 4), \end{cases}$$

οπότε

$$\mathbf{N}(u) \geq 13 \text{ όταν } m \not\equiv 1 (\operatorname{mod} 4) \;\text{ και }\; \mathbf{N}(u) \geq \frac{13}{4} > 3 \text{ όταν } m \equiv 1 (\operatorname{mod} 4)$$

και (κατ' αναλογίαν)

$$\mathbf{N}(v) \geq 13 \text{ όταν } m \not\equiv 1 (\operatorname{mod} 4) \;\text{ και }\; \mathbf{N}(v) > 3 \text{ όταν } m \equiv 1 (\operatorname{mod} 4).$$

Άρα σε κάθε περίπτωση θα ίσχυε

$$\left.\begin{array}{l} \mathbf{N}(u) > 3 \\ \mathbf{N}(v) > 3 \end{array}\right\} \Longrightarrow \mathbf{N}(uv) = \mathbf{N}(u)\mathbf{N}(v) > 9,$$

κάτι που θα αντέκειτο προς το (5.56). Κατά συνέπειαν, $u \in \mathbb{Z}$ (ήτοι $b = 0$) και (λόγω τού (5.55)) $v \in \mathbb{Z}$ (ήτοι $b' = 0$). Επειδή (εξ υποθέσεως) $u \notin \{0, \pm 1\}$ έχουμε

$$\left.\begin{array}{r} u \in \mathbb{Z} \smallsetminus \{0, \pm 1\}, v \in \mathbb{Z} \\ uv = aa' \in \{2, 3\} \end{array}\right\} \Rightarrow u \in \{\pm 2, \pm 3\},\; v \in \{\pm 1\}. \tag{5.57}$$

Εν συνεχεία, εφαρμόζοντας τις συνθήκες διαιρετότητας (5.54) για την *ειδική* τιμή

$$z = \begin{cases} 1 + \sqrt{m}, & \text{όταν } m \not\equiv 1 (\operatorname{mod} 4), \\ \frac{1+\sqrt{m}}{2}, & \text{όταν } m \equiv 1 (\operatorname{mod} 4), \end{cases}$$

λαμβάνουμε (μέσω τού (5.57))

$$\pm 2 \mid z \text{ ή } \pm 2 \mid z - 1 \text{ ή } \pm 2 \mid z + 1 \text{ ή } \pm 3 \mid z \text{ ή } \pm 3 \mid z - 1 \text{ ή } \pm 3 \mid z + 1. \tag{5.58}$$

Εάν υποθέσουμε ότι $\pm 2 \mid z$, τότε θα πρέπει να υπάρχουν $\mu, \nu \in \mathbb{Z}$ με

$$z = \begin{cases} \pm 2(\mu + \nu\sqrt{m}), & \text{όταν } m \not\equiv 1 (\operatorname{mod} 4), \\ \pm 2(\mu + \frac{1+\sqrt{m}}{2}\nu), & \text{όταν } m \equiv 1 (\operatorname{mod} 4), \end{cases}$$

πράγμα αδύνατον, καθόσον $\nexists \nu \in \mathbb{Z} : \pm 2\nu = 1$. Παρομοίως αποδεικνύεται ότι δεν ικανοποιείται καμία εκ των υπολοίπων συνθηκών (5.58). Επομένως καταλήγουμε σε άτοπο! Ως εκ τούτου, η $\mathfrak{O}_m$ δεν είναι ευκλείδεια περιοχή. $\square$

5.5.6 Λήμμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων με $m \equiv 1 (\bmod 4)$. Εάν για οιαδήποτε $z \in \mathfrak{O}_m$ και $w \in \mathfrak{O}_m \smallsetminus \{0\}$, το κλάσμα $\frac{z}{w} = zw^{-1}$, γραφόμενο υπό τη μορφή*

$$\frac{z}{w} = x + \left(\tfrac{1+\sqrt{m}}{2}\right) y = \left(x + \tfrac{y}{2}\right) + \tfrac{y}{2}\sqrt{m} \in \mathbb{Q}(\sqrt{m}), \;\; x, y \in \mathbb{Q}, \tag{5.59}$$

είναι τέτοιο, ώστε να υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη

$$\begin{aligned} \left|\mathbf{N}((a-x) + (b-y)\tfrac{1+\sqrt{m}}{2})\right| &= \left|(a-x)^2 + (a-x)(b-y) - \tfrac{(m-1)(b-y)^2}{4}\right| \\ &= \left|\left((a-x) + \tfrac{1}{2}(b-y)\right)^2 - \tfrac{m(b-y)^2}{4}\right| < 1, \end{aligned} \tag{5.60}$$

τότε η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή.

ΑΠΟΔΕΙΞΗ. Βάσει των προαναφερθέντων στο εδάφιο 5.4.13 αρκεί να αποδειχθεί ότι η απεικόνιση $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii). Προς τούτο θεωρούμε τυχόντα στοιχεία $z \in \mathfrak{O}_m$ και $w \in \mathfrak{O}_m \smallsetminus \{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w} = zw^{-1}$ υπό τη μορφή (5.59). Εξ υποθέσεως, υπάρχουν $a, b \in \mathbb{Z}$ ικανοποιούντες τη συνθήκη (5.37). Θέτοντας

$$q := a + b\tfrac{1+\sqrt{m}}{2} \in \mathfrak{O}_m, \;\; r := z - qw \in \mathfrak{O}_m,$$

παρατηρούμε ότι $z = qw + r$. Στην περίπτωση όπου $r \neq 0$ η (5.37) δίδει

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\mathbf{N}(\frac{z}{w} - q)\right| = \left|\mathbf{N}((a-x) + (b-y)\tfrac{1+\sqrt{m}}{2})\right| < 1,$$

οπότε (λόγω των προαναφερθέντων στο εδάφιο 5.2.40)

$$\left|\mathbf{N}(\frac{r}{w})\right| = \left|\frac{\mathbf{N}(r)}{\mathbf{N}(w)}\right| = \frac{|\mathbf{N}(r)|}{|\mathbf{N}(w)|} = \frac{\boldsymbol{\delta}_{\mathbf{N}}(r)}{\boldsymbol{\delta}_{\mathbf{N}}(w)} < 1 \Rightarrow \boldsymbol{\delta}_{\mathbf{N}}(r) < \boldsymbol{\delta}_{\mathbf{N}}(w).$$

Επομένως, η απεικόνιση $\boldsymbol{\delta}_{\mathbf{N}}$ πληροί τη συνθήκη 5.4.1 (ii) και η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή. □

5.5.7 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m < 0$, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή.*

(ii) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι ευκλείδεια περιοχή.*

(iii) $m \in \{-11, -7, -3, -2, -1\}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Προφανές.

(ii)⇒(iii) Κατά το λήμμα 5.5.5, $m > -13$, δηλαδή

$$m \in \{-11, -10, -7, -6, -5, -3, -2, -1\}.$$

Όταν $m \in \{-10, -6, -5\}$, τότε προφανώς $m \leq -3$, $m \not\equiv 1(\mathrm{mod}\, 4)$ και η ακεραία περιοχή $\mathfrak{O}_m = \mathbb{Z}[\sqrt{m}]$ δεν είναι Π.Κ.Ι. (βλ. πρόταση 5.5.2 και το (iii) τής προτάσεως 5.3.8). Ως εκ τούτου, όταν $m \in \{-10, -6, -5\}$ η $\mathfrak{O}_m = \mathbb{Z}[\sqrt{m}]$ δεν είναι ευκλείδεια περιοχή (βλ. θεώρημα 5.4.21). Άρα $m \in \{-11, -7, -3, -2, -1\}$.

(iii)⇒(i) Επειδή

$$-2 \equiv 2(\mathrm{mod}\, 4), \ -1 \equiv 3(\mathrm{mod}\, 4),$$

έχουμε $\mathfrak{O}_m = \mathbb{Z}[\sqrt{m}]$ όταν $m \in \{-2, -1\}$. Επομένως, για $m \in \{-2, -1\}$ η ακεραία περιοχή $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή επί τη βάσει τής προτάσεως 5.4.16. Έστω τώρα ότι $m \in \{-11, -7, -3\}$. Προφανώς, $m \equiv 1(\mathrm{mod}\, 4)$ και $\mathfrak{O}_m = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Θεωρούμε τυχόντα στοιχεία $z \in \mathfrak{O}_m$ και $w \in \mathfrak{O}_m \smallsetminus \{0\}$ και εκφράζουμε το κλάσμα $\frac{z}{w} = zw^{-1}$ υπό τη μορφή

$$\frac{z}{w} = x + \left(\tfrac{1+\sqrt{m}}{2}\right) y = \left(x + \tfrac{y}{2}\right) + \tfrac{y}{2}\sqrt{m} \in \mathbb{Q}(\sqrt{m}), \ \ x, y \in \mathbb{Q}.$$

Θέτοντας $b := \{y\}_{\varepsilon\gamma\gamma}$ και $a := \{x - \frac{1}{2}(b-y)\}_{\varepsilon\gamma\gamma}$ παρατηρούμε ότι

$$\left|\mathbf{N}((a-x) + (b-y)\tfrac{1+\sqrt{m}}{2})\right| = \left|\left((a-x) + \frac{1}{2}(b-y)\right)^2 - \tfrac{m(b-y)^2}{4}\right| \leq \tfrac{1}{4} + \tfrac{11}{16} < 1.$$

Επομένως, η συνθήκη (5.60) ικανοποιείται και η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή επί τη βάσει τού λήμματος 5.5.6. □

Μέσω τού θεωρήματος 5.5.7 επιτυγχάνεται πλήρης προσδιορισμός όσων εκ των $\mathfrak{O}_m$ είναι ευκλείδειες περιοχές όταν $m < 0$. Αντιθέτως, όταν $m > 1$, είναι γνωστό μόνον το ακόλουθο:

5.5.8 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m > 1$, τότε η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια περιοχή εάν και μόνον εάν*

$$m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

5.5.9 Σημείωση. (i) Ο προσδιορισμός των $\mathbf{N}$-ευκλειδείων περιοχών $\mathfrak{O}_m$ των ακεραίων τού $\mathbb{Q}(\sqrt{m})$ για $m > 1$ διήνυσε μια μακρά ιστορική διαδρομή και απασχόλησε πληθώρα μαθηματικών. Ο Dickson[16] απέδειξε ότι η $\mathfrak{O}_m$ είναι $\mathbf{N}$-ευκλείδεια για $m = 2, 3, 5, 13$ (έχοντας λανθασμένως εικάσει τη μη ύπαρξη άλλων). Ο Perron[17] προσέθεσε στον κατάλογο τους 6, 7, 11, 17, 21 και 29. Εν συνεχεία, οι Oppenheimer, Remak και Rédei προσέθεσαν τους υπολοίπους. (Ο Rédei είκασε

[16]Dickson L.E.: *Algebren und ihre Zahlentheorie*, Orell Füssli Verlag, Zürich und Leipzig, 1927.

[17]Perron O.: *Quadratische Zahlkörper mit Euklidischem Algorithmus*, Math. Annalen 107, (1932), 489-495.

ότι στον κατάλογο θα ανήκει και το 97, κάτι που κατερρίφθη αργότερα μέσω εργασιών των Barnes και Swinnerton-Dyer.) Βεβαίως, το ότι ο προσδιοριστέος κατάλογος είναι *πεπερασμένος* προέκυπτε ήδη από εργασίες τού Heilbronn δημοσιευθείσες στις αρχές τής δεκαετίας τού 1930. Ωστόσο, η συνθήκη τού «μόνο εάν» τού θεωρήματος 5.5.8 απεδείχθη πλήρως από τους Chatland και Davenport[18], και -ανεξαρτήτως- από τον Inkeri[19] στα μέσα τού 20ου αιώνα.

(ii) Στην περίπτωση όπου $m > 1$ (και σε αντίθεση με ό,τι συμβαίνει όταν $m < 0$) υπάρχουν ευκλείδειες περιοχές $\mathfrak{O}_m$ που *δεν είναι* **N**-ευκλείδειες. Επί παραδείγματι, το 1994 ο Clark[20] απέδειξε ότι η $\mathfrak{O}_{69}$ (με $69 \equiv 1(\mathrm{mod}\, 4)$) είναι ευκλείδεια περιοχή με την

$$\boldsymbol{\delta} : \mathfrak{O}_{69} \smallsetminus \{0\} \longrightarrow \mathbb{N}_0, \; \boldsymbol{\delta}\,(z) := \begin{cases} \left|a^2 + ab - 17b^2\right|, & \text{όταν } (a,b) \neq (10,3), \\ 26, & \text{όταν } (a,b) = (10,3), \end{cases}$$

ως ευκλείδεια στάθμη της για κάθε $z = a + \frac{1+\sqrt{69}}{2} b \in \mathfrak{O}_{69}$ $(a, b \in \mathbb{Z})$.

5.5.10 Λήμμα. *Έστω R μια ακεραία περιοχή. Υποθέτουμε ότι υφίσταται απεικόνιση $\boldsymbol{\eta} : R \longrightarrow \mathbb{N}_0$ η οποία ικανοποιεί την εξής συνθήκη: Για κάθε $y \in R \smallsetminus \{0_R\}$ και για κάθε $x \in R$ με $y \nmid x$ υπάρχουν κάποια στοιχεία $u, t \in R$, ούτως ώστε να ισχύουν οι ανισότητες*

$$\boldsymbol{\eta}(0_R) < \boldsymbol{\eta}(xu - yt) < \boldsymbol{\eta}(y). \tag{5.61}$$

Τότε η R είναι Π.Κ.Ι.

ΑΠΟΔΕΙΞΗ. Το τετριμμένο ιδεώδες τής R είναι προφανώς κύριο. Αρκεί λοιπόν να αποδείξουμε ότι και κάθε μη τετριμμένο ιδεώδες τής R είναι κύριο. Υποθέτοντας ότι το I είναι τυχόν μη τετριμμένο ιδεώδες τής R, επιλέγουμε ένα $y \in I \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει

$$\boldsymbol{\eta}\,(y) = \min \{\, \boldsymbol{\eta}\,(z) \mid z \in I \smallsetminus \{0_R\}\} \,.$$

(Το σύνολο $\{\, \boldsymbol{\eta}\,(z) \mid z \in I \smallsetminus \{0_R\}\}$, όντας υποσύνολο τού $\mathbb{N}_0$, διαθέτει ελάχιστο στοιχείο.) Θα αποδείξουμε ότι $I = \langle y \rangle$ κάνοντας χρήση τής «εις άτοπον απαγωγής». Προφανώς, $\langle y \rangle \subseteq I$. Ας υποθέσουμε ότι $\langle y \rangle \subsetneqq I$. Θεωρούμε τυχόν $x \in I \smallsetminus \langle y \rangle$. Επειδή $y \nmid x$, υπάρχουν (εξ υποθέσεως) κάποια στοιχεία $u, t \in R$, ούτως ώστε να ισχύουν οι ανισότητες (5.61). Επομένως,

$$\left. \begin{array}{r} u \in R, x \in I \Rightarrow xu \in I \\ t \in R, y \in I \Rightarrow yt \in I \end{array} \right\} \Rightarrow xu - yt \in I.$$

[18] Chatland H. and Davenport H.: *Euclid's algorithm in real quadratic fields*, Canad. J. Math. **2**, (1950), 289-296.

[19] Inkeri K.: *Über den Euklidischen Algorithmus in quadratischen Zahlkörpern,* Ann. Acad. Scient. Fennicae, Vol. **41** (1947).

[20] Βλ. Clark D.A.: *A quadratic field which is euclidean but not norm-euclidean*, Manuscripta Math. **83**, (1994), 327-330.

Επειδή $\boldsymbol{\eta}(0_R) < \boldsymbol{\eta}(xu - yt)$, έχουμε κατ' ανάγκην $xu - yt \neq 0_R$, οπότε (λόγω τού τρόπου επιλογής τού y)

$$xu - yt \in I \smallsetminus \{0_R\} \Rightarrow \boldsymbol{\eta}(xu - yt) \geq \boldsymbol{\eta}(y).$$

Τούτο μας οδηγεί σε άτοπο (διότι αντίκειται στη δεύτερη εκ των ανισοτήτων (5.61)). Τελικώς λοιπόν $I = \langle y \rangle$ και η R είναι Π.Κ.Ι. □

5.5.11 Λήμμα. *Έστω m ένας αρνητικός ακέραιος αριθμός στερούμενος τετραγώνων. Εάν για κάθε $y \in \mathfrak{O}_m \smallsetminus \{0_R\}$ και για κάθε $x \in \mathfrak{O}_m$ με $y \nmid x$ υπάρχουν κάποια στοιχεία $u, t \in \mathfrak{O}_m$, ούτως ώστε να ισχύουν οι ανισότητες*

$$0 < \mathbf{N}\left(\frac{x}{y}u - t\right) < 1, \tag{5.62}$$

τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού λήμματος 5.5.10 για την ακεραία περιοχή $R = \mathfrak{O}_m$ και για την απεικόνιση

$$\boldsymbol{\eta} : \mathfrak{O}_m \longrightarrow \mathbb{N}_0, \ \ z \longmapsto \boldsymbol{\eta}(z) := \mathbf{N}(z),$$

λαμβανομένων υπ' όψιν των ιδιοτήτων τής αριθμητικής στάθμης $\mathbf{N}$ που έχουν προαναφερθεί στα εδάφια 5.2.39 (i), (v) και 5.2.40. Εν προκειμένω, οι ανισότητες (5.61) είναι ισοδύναμες με τις (5.62). □

5.5.12 Πρόταση. (Gauss) *Εάν $m \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}$, τότε η ακεραία περιοχή $\mathfrak{O}_m$ είναι Π.Κ.Ι.*

ΑΠΟΔΕΙΞΗ. Εάν

$$m \in \{-11, -7, -3, -2, -1\},$$

τότε σύμφωνα με το θεώρημα 5.5.7 η $\mathfrak{O}_m$ είναι ευκλείδεια περιοχή και, ως εκ τούτου, Π.Κ.Ι. (βλ. θεώρημα 5.4.21). Γι' αυτόν τον λόγο θα υποθέσουμε εφεξής ότι

$$m \in \{-163, -67, -43, -19\}.$$

Προφανώς, $m \equiv 1 (\operatorname{mod} 4)$ και $\mathfrak{O}_m = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. Θεωρώντας $y \in \mathfrak{O}_m \smallsetminus \{0_R\}$ και $x \in \mathfrak{O}_m$ με $y \nmid x$ γράφουμε το κλάσμα $\frac{x}{y}$ υπό τη μορφή

$$\frac{x}{y} = \frac{\lambda + \mu\sqrt{m}}{\nu}, \text{ όπου } \lambda, \mu \in \mathbb{Z}, \nu \in \mathbb{N}, \text{ και μκδ}(\lambda, \mu, \nu) = 1.$$

Επειδή

$$y \nmid x \Rightarrow \frac{x}{y} \in \mathbb{Q}(\sqrt{m}) \smallsetminus \mathfrak{O}_m,$$

έχουμε $\nu \geq 2$, όπου $\nu > 2 \Leftrightarrow$ είτε αμφότεροι οι λ, μ είναι άρτιοι είτε αμφότεροι οι λ, μ είναι περιττοί. Αρκεί (λόγω τού λήμματος 5.5.11) να αποδείξουμε ότι υπάρχουν $u, t \in \mathfrak{O}_m$, ούτως ώστε να ισχύουν οι ανισότητες (5.62). Για διευκόλυνσή μας θέτουμε

$$\nu_0 := \begin{cases} 15, & \text{όταν } m = -163, \\ 10, & \text{όταν } m = -67, \\ 8, & \text{όταν } m = -43, \\ 5, & \text{όταν } m = -19, \end{cases}$$

και διαχωρίζουμε περιπτώσεις: *Περίπτωση πρώτη*. Εάν $\boxed{\nu \geq \nu_0,}$ τότε θέτουμε

$$\mathsf{P} := \lambda a + \mu m b - \nu c, \ \ \mathsf{Q} := \lambda b + \mu a + \nu d \tag{5.63}$$

όπου $a, b, c, d \in \mathbb{Z}$, τέτοιοι ώστε $\mathsf{Q} = 1$ και $c := \left\{\frac{\lambda a + \mu m b}{\nu}\right\}_{\varepsilon\gamma\gamma}$. (Αυτή η επιλογή των a, b, d είναι δυνατή, διότι μκδ$(\lambda, \mu, \nu) = 1$.) Εν συνεχεία, ορίζουμε τα u, t ως ακολούθως:

$$u := a + b\sqrt{m} \in \mathfrak{O}_m, \ t := c - d\sqrt{m} \in \mathfrak{O}_m. \tag{5.64}$$

Προφανώς,

$$\frac{xu - yt}{y} = \frac{x}{y}u - t = \frac{\mathsf{P} + \mathsf{Q}\sqrt{m}}{\nu} = \frac{\mathsf{P}}{\nu} + \frac{1}{\nu}\sqrt{m}$$

και

$$\left.\begin{array}{r} (5.51) \Rightarrow \mathbf{N}\left(xu - yt\right) \geq 0, \ \mathbf{N}\left(y\right) > 0 \\ \frac{\mathbf{N}(xu-yt)}{\mathbf{N}(y)} = \mathbf{N}\left(\frac{xu-yt}{y}\right) = \mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2 - m}{\nu^2} \\ \sqrt{m} \notin \mathbb{Q} \Rightarrow m \neq \mathsf{P}^2 \end{array}\right\} \Rightarrow \mathbf{N}\left(\frac{x}{y}u - t\right) > 0. \tag{5.65}$$

Από την άλλη μεριά,

$$\left|\frac{\mathsf{P}}{\nu}\right| = \left|\frac{\lambda a + \mu m b}{\nu} - c\right| \leq \frac{1}{2}, \tag{5.66}$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2 - m}{\nu^2} \leq \frac{1}{4} - \frac{m}{\nu^2}.$$

Όταν $-m < \frac{3}{4}\nu_0^2$, τότε

$$-m < \frac{3}{4}\nu_0^2 < \frac{3}{4}\nu^2 \Rightarrow \mathbf{N}\left(\frac{x}{y}u - t\right) < 1. \tag{5.67}$$

Τούτο είναι αληθές για τις πρώτες τρεις τιμές τού m:

$-m$	163	67	43
$\frac{3}{4}\nu_0^2$	$168,75$	75	48

Όταν $m = -19$, τότε για $\nu \geq 6$ έχουμε

$$-m = 19 < 27 = \frac{3}{4}6^2 < \frac{3}{4}\nu^2 \Rightarrow \mathbf{N}\left(\frac{x}{y}u - t\right) < 1. \tag{5.68}$$

Για $\nu = \nu_0 = 5$ η (5.66) δίδει

$$\left.\begin{array}{r} |\mathsf{P}| \leq \frac{5}{2} \\ |\mathsf{P}| \in \mathbb{N}_0 \end{array}\right\} \Rightarrow |\mathsf{P}| \leq 2 \Rightarrow \mathsf{P}^2 \leq 4 \Rightarrow \mathsf{P}^2 + 19 \leq 23 < 25,$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2 + 19}{25} < 1. \tag{5.69}$$

Λόγω των (5.65), (5.67), (5.68) και (5.69) οι ανισότητες (5.62) ισχύουν για τα επιλεχθέντα u, t.

Περίπτωση δεύτερη. Εάν $\boxed{\nu = 4 \text{ και αμφότεροι } \lambda, \mu \text{ περιττοί,}}$ τότε

$$\exists \xi, \varrho \in \mathbb{Z} : \lambda = 2\xi + 1, \;\; \mu = 2\varrho + 1.$$

Ορίζουμε τα u, t ως ακολούθως:

$$u := \frac{\lambda - \mu\sqrt{m}}{2} \in \mathfrak{O}_m, \; t := \frac{\lambda^2 - m\mu^2 - 4}{8} \in \mathfrak{O}_m.$$

Σημειωτέον ότι $t \in \mathbb{Z}$, διότι $8 \mid 4\xi\,(\xi + 1)\,,\; 8 \mid 4\varrho\,(\varrho + 1)\,,$

m	-163	-67	-43	-19
$-m-3$	160	64	40	16

και

$$\lambda^2 - m\mu^2 - 4 = 4\xi\,(\xi + 1) - 4\varrho\,(\varrho + 1) - m - 3.$$

Επιπροσθέτως,

$$\frac{x}{y}u - t = \left(\frac{\lambda + \mu\sqrt{m}}{4}\right)\left(\frac{\lambda - \mu\sqrt{m}}{2}\right) - t = \frac{1}{2},$$

οπότε

$$0 < \mathbf{N}\left(\frac{x}{y}u - t\right) = \mathbf{N}\left(\frac{1}{2}\right) = \frac{1}{4} < 1.$$

Άρα για τα επιλεχθέντα u, t ισχύουν οι ανισότητες (5.62).

Περίπτωση τρίτη. Εάν $\boxed{\nu < \nu_0 \text{ και τουλάχιστον ένας εκ των } \lambda, \mu \text{ άρτιος για } \nu = 4,}$ τότε αξιώνουμε από τα u, t να έχουν την μορφή (5.64) και από τα P και Q να είναι βραχυγραφίες όπως στη (5.63), αλλά τούτη τη φορά με τους $a, b, d \in \mathbb{Z}$ οριζόμενους ως εξής:

$$a := \lambda, \;\; b := -\mu, \;\; d := 0$$

και τον $c \in \mathbb{Z}$ επιλεγμένον κατά τέτοιον τρόπο, ώστε

$$\frac{\lambda^2 - m\mu^2}{\nu} \geq c > \frac{\lambda^2 - m\mu^2}{\nu} - 1.$$

Προφανώς, $\mathsf{Q} = 0$, $\mathsf{P} = \lambda^2 - m\mu^2 - \nu c$ με $0 \leq \mathsf{P} < \nu$ και

$$\frac{x}{y}u - t = \frac{\mathsf{P} + \mathsf{Q}\sqrt{m}}{\nu} = \frac{\lambda^2 - m\mu^2 - \nu c}{\nu} = \frac{\lambda^2 - m\mu^2}{\nu} - c,$$

οπότε

$$\mathbf{N}\left(\frac{x}{y}u - t\right) = \frac{\mathsf{P}^2}{\nu^2} < 1.$$

Για να ισχύουν αμφότερες οι ανισότητες (5.62) για τα επιλεχθέντα u, t αρκεί, ως εκ τούτου, να αποδειχθεί ότι $\mathsf{P} \neq 0$. Τούτο έπεται από την

$$\lambda^2 - m\mu^2 \not\equiv 0 (\operatorname{mod} \nu). \tag{5.70}$$

Η (5.70) είναι αληθής όταν $\nu = 2$ ή $\nu = 4$ (όπου στη δεύτερη τιμή λαμβάνουμε υπ' όψιν την επιπρόσθετη προϋπόθεσή μας), διότι *είτε* ο λ είναι άρτιος και ο μ περιττός *είτε* ο λ είναι περιττός και ο μ άρτιος (αφού μκδ$(\lambda, \mu, \nu) = 1$). Η (5.70) είναι αληθής ακόμη και όταν $\nu = 8 = 2^3$, διότι τουλάχιστον ο ένας εκ των λ, μ είναι περιττός, οπότε

$$\lambda^2 - m\mu^2 \equiv \lambda^2 + 3\mu^2 \equiv \begin{cases} 4 (\operatorname{mod} 8), & \text{όταν } \lambda \equiv \mu \equiv 1 (\operatorname{mod} 2), \\ 1 (\operatorname{mod} 2), & \begin{array}{l} \text{όταν } \lambda \equiv 1 (\operatorname{mod} 2), \; \mu \equiv 0 (\operatorname{mod} 2) \\ \text{ή } \lambda \equiv 0 (\operatorname{mod} 2), \; \mu \equiv 1 (\operatorname{mod} 2). \end{array} \end{cases}$$

Για τις εναπομείνασες περιπτώσεις, όπου το ν έχει ως διαιρέτη του κάποιον πρώτο αριθμό p, $2 < p \leq \nu < \nu_0$, η επαλήθευση τής (5.70) ανάγεται στην επαλήθευση των ακολούθων:

$$\lambda^2 - m\mu^2 \not\equiv 0 (\operatorname{mod} p), \;\; \forall p \in \Xi,$$

όπου $\Xi := \{p | p$ πρώτος $\geq 3,\ p \mid \nu\}$. Επειδή (εξ υποθέσεως) $\nu < \nu_0$, το Ξ είναι (κατά περίπτωση) το εξής:

m	-163	-67	-43	-19
ν_0	15	10	8	5
Ξ	$\{3,5,7,11,13\}$	$\{3,5,7\}$	$\{3,5,7\}$	$\{3\}$

Θα εργασθούμε με «εις άτοπον απαγωγή». Ας υποθέσουμε ότι υπάρχει κάποιος $p \in \Xi$, τέτοιος ώστε

$$\lambda^2 - m\mu^2 \equiv 0(\mathrm{mod}\, p).$$

Εάν το p ήταν διαιρέτης τού μ, τότε θα ήταν διαιρέτης και τού λ, πράγμα αδύνατον αφού μκδ$(\lambda, \mu, \nu) = 1$. Άρα μκδ$(\mu, p) = 1$, οπότε (λόγω τής προτάσεως 3.4.1)

$$\exists \mu' \in \mathbb{Z} : \mu\mu' \equiv 1(\mathrm{mod}\, p).$$

Έστω $\kappa := \lambda\mu'$. Τότε

$$\lambda^2 - m\mu^2 \equiv 0(\mathrm{mod}\, p) \Rightarrow \left(\lambda^2 - m\mu^2\right)(\mu')^2 \equiv 0(\mathrm{mod}\, p) \Rightarrow \kappa^2 \equiv m(\mathrm{mod}\, p). \quad (5.71)$$

Αρκεί να αποδείξουμε ότι η ισοτιμία (5.71) είναι αναληθής για όλους τους δυνατούς πρώτους αριθμούς $p \geq 3$.

(i) Εάν $p = 3$, τότε $m \in \{-163, -67, -43, -19\}$ με $m \equiv 2(\mathrm{mod}\, 3)$, ενώ $\kappa^2 \equiv 0$ ή $1(\mathrm{mod}\, 3)$.

(ii) Εάν $p = 5$, τότε έχουμε $m \in \{-163, -67, -43\}$ με $-163,\ -43 \equiv 2(\mathrm{mod}\, 5)$ και $-67 \equiv 3(\mathrm{mod}\, 5)$, ενώ $\kappa^2 \equiv 0, 1$ ή $4(\mathrm{mod}\, 5)$.

(iii) Εάν $p = 7$, τότε $m \in \{-163, -67, -43\}$ με $-163 \equiv 5(\mathrm{mod}\, 7)$, $-67 \equiv 3(\mathrm{mod}\, 7)$ και $-43 \equiv 6(\mathrm{mod}\, 7)$, ενώ $\kappa^2 \equiv 0, 1, 4$ ή $2(\mathrm{mod}\, 7)$.

(iv) Εάν $p = 11$, τότε $m = -163 \equiv 2(\mathrm{mod}\, 11)$, ενώ $\kappa^2 \equiv 0, 1, 4, 9, 5$ ή $3(\mathrm{mod}\, 11)$.

(v) Εάν $p = 13$, τότε $m = -163 \equiv 6(\mathrm{mod}\, 13)$, ενώ $\kappa^2 \equiv 0, 1, 4, 9, 3, 12$ ή $10(\mathrm{mod}\, 13)$.

Εδώ περατούται η απόδειξη τής προτάσεως. □

5.5.13 Πόρισμα. *Εάν $m \in \{-163, -67, -43, -19\}$, τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι. αλλά δεν είναι ευκλείδεια περιοχή.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 5.5.7 και την πρόταση 5.5.12. □

Η πρόταση 5.5.12 ισχυροποιείται κατά τρόπο ουσιαστικό ως ακολούθως:

5.5.14 Θεώρημα. *Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Εάν $m < 0$, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η ακεραία περιοχή $\mathfrak{O}_m$ είναι Π.Κ.Ι.*

(ii) $m \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}$.

5.5.15 Σημείωση. (i) Αριθμητικές μαρτυρίες και υπολογισμοί για το ότι οι ανωτέρω εννέα αριθμοί m είναι οι *μόνοι* «υποψήφιοι», ούτως ώστε οι αντίστοιχες ακέραιες περιοχές $\mathfrak{O}_m$ να είναι Π.Κ.Ι., εντοπίζονται ήδη στα έργα τού C.-F. Gauss και άλλων μαθηματικών τής εποχής του. Το έτος 1934 οι Heilbronn και Linfoot[21] διεπίστωσαν ότι, στην περίπτωση που θα υπήρχε αρνητικός ακέραιος m στερούμενος τετραγώνων (διαφορετικός των ανωτέρω εννέα) με αυτήν την ιδιότητα, ο $|m|$ θα όφειλε να είναι πολύ μεγάλος. Το 1952 Heegner[22] έδωσε μία απόδειξη τού αδυνάτου τής υπάρξεως τέτοιου αριθμού, η οποία όμως περιείχε ορισμένα λάθη. Οι πρώτες ορθές αποδείξεις οφείλονται στους Baker[23] και Stark[24] (στα μέσα τής δεκαετίας τού 1960). Τέλος, το 1968 οι Birch[25], Deuring[26] και Siegel[27] κατόρθωσαν να διορθώσουν ακόμη και τα λάθη τής αρχικής αποδείξεως τού Heegner.

(ii) Ένα θεώρημα ανάλογο τού 5.5.14 δεν έχει -μέχρι στιγμής- αποδειχθεί για *θετικούς* m. Ωστόσο, υπάρχουν αρκετά χρήσιμα αποτελέσματα υπολογιστικής φύσεως. Επί παραδείγματι, οι (στερούμενοι τετραγώνων) αριθμοί

$$\begin{gathered}2,3,5,6,7,11,13,14,17,19,21,22,23,29,\\ 31,33,37,38,41,43,46,47,53,57,59,61,\\ 62,,67,69,71,73,77,83,86,89,93,94 \text{ και } 97\end{gathered}$$

είναι οι μόνοι m, $1 < m \leq 100$, για τους οποίους η $\mathfrak{O}_m$ είναι Π.Κ.Ι. Ακόμη και το *φυσικό ερώτημα* τού κατά πόσον υπάρχουν *άπειροι* θετικοί m με αυτήν την ιδιότητα δεν έχει εισέτι απαντηθεί.

5.5.16 Πόρισμα. *Έστω m ένας ακέραιος στερούμενος τετραγώνων. Εάν $m < 0$, τότε η $\mathfrak{O}_m$ είναι Π.Κ.Ι. και μη ευκλείδεια περιοχή εάν και μόνον εάν*

$$m \in \{-163, -67, -43, -19\}.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τα θεωρήματα 5.5.7 και 5.5.14. □

[21]Heilbronn H. and Linfoot E.H.: *On the imaginary quadratic corpora of class-number one*, Quart. J. Math. (Oxford), Vol. **5**, (1934), 293-301.

[22]Heegner K.: *Diophantische Analysis und Modulfunktionen*, Math. Z. **56**, (1952), 227-253.

[23]Baker A.: *Linear forms in the logarithms of algebraic numbers*, Mathematika **13**, (1966), 204-216.

[24]Stark H.M.: *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14**, (1967), 1-27.

[25]Birch B.J.: *Diophantine analysis and modular functions*, Proc. Conf. in Algebraic Geometry, Tata Institute, Bombay, (1968), 35-42.

[26]Deuring M: *Imaginäre quadratische Zahlkörper mit Klassenzahl Eins*, Invent. Math. **5**, (1968), 169-179.

[27]Siegel C.L.: *Zum Beweise des Starkschen Satzes*, Invent. Math. **5**, (1968), 180-191.

5.6 ΠΕΡΙΟΧΕΣ ΜΟΝΟΣΗΜΑΝΤΗΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΕΩΣ

5.6.1 Ορισμός. Μια ακεραία περιοχή R καλείται **περιοχή με παραγοντοποίηση** όταν κάθε $a \in R \smallsetminus (R^\times \cup \{0_R\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων τής R, ήτοι όταν γράφεται υπό τη μορφή

$$a = uq_1q_2\cdots q_k,$$

όπου $u \in R^\times$, $k \in \mathbb{N}$ και τα $q_1, q_2, \ldots, q_k$ είναι ανάγωγα στοιχεία τής R.

5.6.2 Ορισμός. Μια ακεραία περιοχή R καλείται **περιοχή μονοσήμαντης παραγοντοποιήσεως (=: Π.Μ.Π.)** όταν πληροί τις ακόλουθες συνθήκες:

(i) Η R είναι περιοχή με παραγοντοποίηση (υπό την έννοια τού 5.6.1) και

(ii) για οιεσδήποτε παραστάσεις

$$a \underset{\text{συν.}}{\sim} q_1q_2\cdots q_k \underset{\text{συν.}}{\sim} q_1'q_2'\cdots q_l'$$

συντρόφων ενός $a \in R \smallsetminus (R^\times \cup \{0_R\})$ ως γινομένων πεπερασμένου πλήθους αναγώγων στοιχείων τής R, έχουμε $k = l$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_k$ τού συνόλου $\{1, \ldots, k\}$, τέτοια ώστε να ισχύει

$$q_{\sigma(j)} \underset{\text{συν.}}{\sim} q_j', \quad \forall j \in \{1, \ldots, k\}.$$

5.6.3 Θεώρημα. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η R είναι περιοχή με παραγοντοποίηση και κάθε στοιχείο $q \in R \smallsetminus (R^\times \cup \{0_R\})$ είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

(iii) *Κάθε $a \in R \smallsetminus (R^\times \cup \{0_R\})$ διαθέτει κάποιον σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους πρώτων στοιχείων τής R.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Λόγω τού (iii) τής προτάσεως 5.3.4 αρκεί να αποδείξουμε ότι κάθε ανάγωγο στοιχείο $r \in R \smallsetminus (R^\times \cup \{0_R\})$ είναι πρώτο στοιχείο τής R. Ας υποθέσουμε ότι υπάρχουν $a, b \in R$, τέτοια ώστε να ισχύει $r \mid ab$. Τότε υπάρχει $c \in R$ με $ab = rc$. Γράφοντας τα a, b, c ως

$$a = uq_1q_2\cdots q_k, \quad b = u'q_1'q_2'\cdots q_l', \quad c = u''q_1''q_2''\cdots q_m'',$$

ήτοι ως συντρόφους γινομένων πεπερασμένου πλήθους αναγώγων στοιχείων τού R (όπου $u, u', u'' \in R^\times$), λαμβάνουμε

$$uu'\,(\prod_{j=1}^{k} q_j)\,(\prod_{\varrho=1}^{l} q_\varrho') = ab = u''\,r\,q_1''q_2''\cdots q_m''.$$

Επειδή η R είναι Π.Μ.Π., είτε υπάρχει $j \in \{1, \ldots, k\}$ με $r \underset{\text{συν.}}{\sim} q_j$ είτε υπάρχει $\varrho \in \{1, \ldots, l\}$ με $r \underset{\text{συν.}}{\sim} q'_\varrho$. Κατά συνέπειαν, είτε $r \mid a$ είτε $r \mid b$.

(ii)⇒(iii): Τούτο είναι προφανές.

(iii)⇒(i): Έστω τυχόν $a \in R \smallsetminus (R^\times \cup \{0_R\})$. Εξ υποθέσεως υπάρχουν $\in R^\times$ και πρώτα στοιχεία $p_1, \ldots, p_k$, τέτοια ώστε

$$a = up_1p_2 \cdots p_k.$$

Επειδή κάθε πρώτο στοιχείο τής R είναι ανάγωγο (βλ. 5.3.4 (iii)), η R πληροί τη συνθήκη (i) τού ορισμού 5.6.2. Εάν το a διαθέτει μια δεύτερη παράσταση

$$a = wq_1q_2 \cdots q_l,$$

όπου $w \in R^\times$ και τα $q_1, \ldots, q_l$ ανάγωγα στοιχεία τής R, τότε

$$\left.\begin{array}{r} p_1 \mid p_1p_2 \cdots p_k = u^{-1}wq_1q_2 \cdots q_l \\ p_1 \text{ πρώτο, } p_1 \nmid u^{-1},\ p_1 \nmid w \end{array}\right\} \Longrightarrow \exists j_1 \in \{1, \ldots, l\} : p_1 \mid q_{j_1}.$$

Επειδή το q_{j_1} είναι ανάγωγο και το p_1 δεν είναι αντιστρέψιμο, έχουμε $p_1 \underset{\text{συν.}}{\sim} q_{j_1}$, ήτοι $p_1 = eq_{j_1}$ για κάποιο $e \in R^\times$. Ύστερα από απλοποίηση τού p_1 στην ανωτέρω ισότητα λαμβάνουμε

$$\left.\begin{array}{r} p_2 \mid p_2 \cdots p_k = e^{-1}u^{-1}w(\prod\limits_{\varrho \in \{1,..,l\} \smallsetminus \{j_1\}} q_\varrho) \\ \\ p_2 \text{ πρώτο στοιχείο, } p_2 \nmid e^{-1},\ p_2 \nmid u^{-1},\ p_2 \nmid w \end{array}\right\} \Rightarrow \exists j_2 \in \{1,..,l\} \smallsetminus \{j_1\} : p_2 \mid q_{j_2},$$

οπότε και πάλι $p_2 \underset{\text{συν.}}{\sim} q_{j_2}$. Εφαρμόζοντας την ίδια συλλογιστική συμπεραίνουμε ότι $k \leq l$ (έπειτα από k εν συνόλω βήματα) και ότι

$$\exists \{j_1, j_2, \ldots, j_k\} \subseteq \{1, \ldots, l\} : p_\varrho \underset{\text{συν.}}{\sim} q_{j_\varrho},\ \forall \varrho \in \{1, \ldots, k\}.$$

Εάν ίσχυε η ανισότητα $k < l$, τότε θα είχαμε

$$\underbrace{1_R = c\,(\prod_{\varrho \in \{1,..,l\} \smallsetminus \{j_1,..,j_k\}} q_\varrho),\ \text{για κάποιο } c \in R^\times}$$
$$\Downarrow$$
$$\exists \varrho \in \{1,..,l\} \smallsetminus \{j_1,..,j_k\} : q_\varrho \mid 1 \Longrightarrow q_\varrho \in R^\times,$$

πράγμα άτοπο. Συνεπώς, $k = l$, και ορίζοντας τη μετάταξη $\sigma \in \mathfrak{S}_k$ μέσω τού τύπου $\sigma(\varrho) = j_\varrho$ για κάθε $\varrho \in \{1, \ldots, k\}$ λαμβάνουμε $p_\varrho \underset{\text{συν.}}{\sim} q_{\sigma(\varrho)}$. Άρα η R πληροί *και* τη συνθήκη (ii) τού ορισμού 5.6.2, οπότε η R είναι όντως μια Π.Μ.Π. □

5.6.4 Ορισμός. Λέμε ότι μια ακεραία περιοχή R πληροί τη **συνθήκη των αλυσίδων γνησίων διαιρετών** όταν κάθε ανιούσα αλυσίδα *κυρίων ιδεωδών*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

τής R είναι *στάσιμη*, ήτοι όταν $\exists k \in \mathbb{N}$, για τον οποίο ισχύει $I_n = I_k$ για κάθε φυσικό αριθμό $n \geq k$. Η συνθήκη αυτή ισοδυναμεί με την ακόλουθη: Δεν υπάρχει καμία (άπειρη) ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R, τέτοια ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$. (Σημειωτέον ότι, λόγω των (i), (ii) και (iv) τής προτάσεως 5.2.4 και τού ορισμού των γνησίων διαιρετών (βλ. 5.2.8), ο $b \in R$ είναι ένας γνήσιος διαιρέτης ενός $a \in R$ εάν και μόνον εάν $\langle a \rangle \subsetneqq \langle b \rangle \subsetneqq R$)

5.6.5 Θεώρημα. *Έστω R μια ακεραία περιοχή. Εάν υποθέσουμε ότι η R πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, τότε η R είναι περιοχή με παραγοντοποίηση.*

ΑΠΟΔΕΙΞΗ. Έστω

$$\Lambda := \left\{ a \in R \smallsetminus \left(R^{\times} \cup \{0_R\}\right) \;\middle|\; \begin{array}{c} \nexists c \underset{\text{συν.}}{\sim} a \text{ παριστώμενος} \\ \text{ως γινόμενο πεπερασμένου πλήθους} \\ \text{αναγώγων στοιχείων τής } R. \end{array} \right\}.$$

Ας υποθέσουμε ότι η R πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, ότι $\Lambda \neq \varnothing$ κι ας θέσουμε για κάθε $a \in \Lambda$,

$$\Gamma_a := \{\, b \in \Lambda \mid b \text{ είναι γνήσιος διαιρέτης τού } a \}\,.$$

Τότε $\Gamma_a \neq \varnothing$ για οιοδήποτε $a \in \Lambda$. (Πράγματι· εάν υπήρχε $a \in \Lambda$, για το οποίο θα είχαμε $\Gamma_a = \varnothing$, τότε το ίδιο το a θα όφειλε να είναι ανάγωγο, κάτι που θα αντέκειτο προς την υπόθεσή μας.) Σύμφωνα με το αξίωμα τής επιλογής,

$$(\Gamma_a \neq \varnothing,\ \forall a \in \Lambda) \Longrightarrow \prod_{a\in\Lambda} \Gamma_a \neq \varnothing,$$

οπότε υπάρχει μια απεικόνιση

$$f : \Lambda \longrightarrow \bigcup_{a\in\Lambda} \Gamma_a, \quad \text{με } f(a) \in \Gamma_a,\ \forall a \in \Lambda,$$

ήτοι τέτοια, ώστε η εικόνα $f(a)$ τού a μέσω τής f να είναι γνήσιος διαιρέτης τού $a, \forall a \in \Lambda$. Επιλέγοντας ένα τυχόν στοιχείο τού Λ και ονομάζοντάς το a_1 έχουμε τη δυνατότητα να ορίσουμε μια αναδρομική απεικόνιση $\psi : \mathbb{N} \longrightarrow \Lambda$ μέσω των τύπων

$$\psi(1) := a_1, \quad \psi(n+1) := f(\psi(n)) =: a_{n+1},\ \forall n \in \mathbb{N}.$$

Η κατ' αυτόν τον τρόπο σχηματιζομένη ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R είναι τέτοια, ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$. Ως εκ τούτου, η R δεν μπορεί να πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών, κάτι που αντιφάσκει προς την υπόθεσή μας! Άρα τελικώς $\Lambda = \varnothing$ και η R είναι πράγματι περιοχή με παραγοντοποίηση. □

5.6.6 Πόρισμα. *Κάθε ναιτεριανή περιοχή είναι περιοχή με παραγοντοποίηση.*

ΑΠΟΔΕΙΞΗ. Κάθε ναιτεριανή περιοχή πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών (διότι πληροί τη συνθήκη των ανιουσών αλυσίδων επί τού συνόλου *όλων* των ιδεωδών της) και είναι, ως εκ τούτου, περιοχή με παραγοντοποίηση (λόγω τού θεωρήματος 5.6.5). □

5.6.7 Παραδείγματα. (i) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Τότε η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{m}]$, ούσα ναιτεριανή (βλ. πρόταση 4.1.13), είναι περιοχή με παραγοντοποίηση. Ωστόσο, όταν $m \equiv 1 (\mathrm{mod}\, 4)$ ή $m \leq -3$, η $\mathbb{Z}[\sqrt{m}]$ *δεν είναι* Π.Μ.Π.! (Βλ. 5.3.8 (i) και (ii), και 5.6.3 (i)⇒(ii).)

(ii) Υποδακτύλιοι περιοχών μονοσήμαντης παραγοντοποιήσεως δεν είναι απαραιτήτως Π.Μ.Π. Επί παραδείγματι, η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-3}]$ δεν είναι Π.Μ.Π., αλλά αποτελεί υποδακτύλιο τού σώματος $\mathbb{Q}(\sqrt{-3})$ (που είναι Π.Μ.Π.).

5.6.8 Πόρισμα. *Κάθε Π.Κ.Ι. είναι Π.Μ.Π.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα Π.Κ.Ι. Επειδή η R είναι ναιτεριανή, κάθε στοιχείο $a \in R \smallsetminus (R^\times \cup \{0_R\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων τής R (βάσει τού πορίσματος 5.6.6). Χρησιμοποιώντας τό γεγονός τού ότι κάθε ανάγωγο στοιχείο μιας Π.Κ.Ι. είναι πρώτο, καθώς και την ισοδυναμία των (i) και (iii) τού θεωρήματος 5.6.3, συμπεραίνουμε ότι η R οφείλει να είναι περιοχή μονοσήμαντης παραγοντοποιήσεως. □

5.6.9 Ορισμός. Έστω R μια Π.Μ.Π. και έστω $r \in R \smallsetminus \{0_R\}$. Τότε το r είτε είναι αντιστρέψιμο είτε γράφεται ως

$$r = us_1 s_2 \cdots s_k,$$

όπου $u \in R^\times$, $k \in \mathbb{N}$ και τα $s_1, s_2, \ldots, s_k$ πρώτα (= ανάγωγα) στοιχεία τής R. Εάν $s_1 = s_2 = \cdots = s_k =: p$, τότε $r = up^k$. Ειδάλλως, για να συμπτύξουμε σε αυτό το γινόμενο όσα εκ των $s_1, s_2, \ldots, s_k$ είναι πολλαπλώς εμφανιζόμενα (με την εισαγωγή «δυνάμεων») μπορούμε (πιθανώς ύστερα από μια αναδιάταξη δεικτών) να υποθέσουμε ότι

$$s_1 = \cdots = s_{j_1} < s_{j_1+1} = \cdots = s_{j_2} < s_{j_2+1} = \cdots = s_{j_3} < \cdots\cdots < s_{j_{\ell-1}+1} \cdots = s_{j_\ell} = s_k$$

για κατάλληλα $\{j_1, j_2, \ldots, j_\ell\} \subseteq \{1, \ldots, k\},\ 2 \leq l \leq k$, με

$$1 = j_1 < j_2 < \cdots < j_{\ell-1} < j_\ell = k.$$

Θέτοντας

$$\nu_1 := j_1,\ \nu_2 := j_2 - j_1,\ \ldots,\ \nu_\ell := j_\ell - j_{\ell-1},\quad p_\mu := s_{j_\mu},\ \forall \mu \in \{1, \ldots, \ell\},$$

το r γράφεται ως

$$\boxed{r = up_1^{\nu_1} p_2^{\nu_2} \cdots p_\ell^{\nu_\ell}.} \tag{5.72}$$

Η έκφραση (5.72) καλείται **παράσταση τού r ως γινομένου πρώτων στοιχείων** ή **αποσύνθεση τού r σε γινόμενο πρώτων στοιχείων**. Το r μπορεί να γραφεί υπό μία ακόμη πιο βολική μορφή στην οποία *συμπεριλαμβάνεται και η περίπτωση κατά την οποία* $r \in R^\times$, ως ακολούθως: Το σύνολο των πρώτων (= αναγώγων) στοιχείων τής R αποσυντίθεται σε κλάσεις ισοδυναμίας ως προς τη σχέση “ $\underset{\text{συν.}}{\sim}$ ”, ήτοι σε σαφώς διακεκριμένες κλάσεις συντροφικών πρώτων στοιχείων. Έστω $\mathcal{P}_R$ ένα *πλήρες σύστημα εκπροσώπων* αυτών των κλάσεων ισοδυναμίας (ήτοι ένα υποσύνολο τού συνόλου των πρώτων στοιχείων τής R, το οποίο περιέχει *ακριβώς ένα* στοιχείο από καθεμιά εξ αυτών). Τότε

$$\boxed{r = u \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)},\ \ u \in R^\times,} \tag{5.73}$$

όπου

$$\boldsymbol{\nu}_p(r) := \begin{cases} \max\left\{k \in \mathbb{N} \,:\, p^k \mid r\right\}, & \text{όταν } p \mid r, \\ 0, & \text{όταν } p \nmid r. \end{cases}$$

5.6.10 Πρόταση. *Έστω R μια Π.Μ.Π. Εάν $r, s \in R \smallsetminus \{0_R\}$, τότε ισχύουν τα ακόλουθα:*

(i) $\boldsymbol{\nu}_p(rs) = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R.$

(ii) $r \mid s \Longleftrightarrow \boldsymbol{\nu}_p(r) \leq \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R.$

(iii) $r \underset{\text{συν.}}{\sim} s \Longleftrightarrow \boldsymbol{\nu}_p(r) = \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R.$

(iv) $r \in R^\times \Longleftrightarrow \boldsymbol{\nu}_p(r) = 0,\ \forall p \in \mathcal{P}_R.$

(v) *Εάν $r + s \neq 0_R$, τότε $\boldsymbol{\nu}_p(r+s) \geq \min\{\boldsymbol{\nu}_p(r), \boldsymbol{\nu}_p(s)\},\ \forall p \in \mathcal{P}_R.$*

(vi) *Εάν $\boldsymbol{\nu}_p(r) < \boldsymbol{\nu}_p(s)$ για κάποιο $p \in \mathcal{P}_R$, τότε $\boldsymbol{\nu}_p(r+s) = \boldsymbol{\nu}_p(r).$*

ΑΠΟΔΕΙΞΗ. (i) Εάν οι

$$r = u \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)},\ \ s = w \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)}, \tag{5.74}$$

είναι οι παραστάσεις των r και s ως γινομένων πρώτων στοιχείων, τότε, λόγω τού μονοσημάντου τής παραστάσεως τού rs, έχουμε

$$rs = uw \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)+\boldsymbol{\nu}_p(s)} \Longrightarrow \boldsymbol{\nu}_p(rs) = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(s),\ \forall p \in \mathcal{P}_R.$$

(ii) Εάν $r \mid s$, τότε $\exists r' \in R : s = rr'$, οπότε

$$\left.\begin{array}{r}\text{(i)} \Rightarrow \boldsymbol{\nu}_p(s) = \boldsymbol{\nu}_p(rr') = \boldsymbol{\nu}_p(r) + \boldsymbol{\nu}_p(r'),\ \forall p \in \mathcal{P}_R \\ \boldsymbol{\nu}_p(r') \geq 0,\ \forall p \in \mathcal{P}_R\end{array}\right\} \Rightarrow \boldsymbol{\nu}_p(s) \geq \boldsymbol{\nu}_p(r),\ \forall p \in \mathcal{P}_R.$$

(iii) Αυτό έπεται άμεσα από το (ii).

(iv) Εάν $r \in R^{\times}$, τότε $r \underset{\text{συν.}}{\sim} 1$, οπότε εφαρμόζοντας το (iii) λαμβάνουμε

$$\boldsymbol{\nu}_p(r) = \boldsymbol{\nu}_p(1) = 0,\ \forall p \in \mathcal{P}_R.$$

Το αντίστροφο είναι προφανές.

(v) Εάν υποθέσουμε ότι $r + s \neq 0_R$, $\mu_p := \min\{\boldsymbol{\nu}_p(r), \boldsymbol{\nu}_p(s)\}$ και ότι οι (5.74) είναι οι οι παραστάσεις των r και s ως γινομένων πρώτων στοιχείων, τότε

$$r + s = \prod_{p \in \mathcal{P}_R} p^{\mu_p} \left(u \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)-\mu_p} + w \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)-\mu_p} \right),$$

οπότε $\boldsymbol{\nu}_p(r+s) \geq \mu_p,\ \forall p \in \mathcal{P}_R$.

(vi) Ας διατηρήσουμε τους συμβολισμούς τους εισαχθέντες στο (v). Εάν ισχύει η ανισότητα $\boldsymbol{\nu}_p(r) < \boldsymbol{\nu}_p(s)$ για κάποιο $p \in \mathcal{P}_R$, τότε $\mu_p = \boldsymbol{\nu}_p(r)$, πράγμα που σημαίνει ότι

$$p \nmid u \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(r)-\mu_p}, \quad p \mid w \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(s)-\mu_p}.$$

Άρα $\boldsymbol{\nu}_p(r+s) = \boldsymbol{\nu}_p(r)$. □

5.6.11 Θεώρημα. *Εάν μια ακεραία περιοχή R είναι Π.Μ.Π., τότε η R είναι περιοχή με μ.κ.δ. Επιπροσθέτως, εάν $n \in \mathbb{N}$, $n \geq 2$, και $a_1, a_2, \ldots, a_n \in R \smallsetminus \{0_R\}$, τότε*

$$\boxed{\prod_{p \in \mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a_1), \boldsymbol{\nu}_p(a_2), \ldots, \boldsymbol{\nu}_p(a_n)\}} \in \text{ΜΚΔ}_R(a_1, \ldots, a_n)} \tag{5.75}$$

και

$$\boxed{\prod_{p \in \mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a_1), \boldsymbol{\nu}_p(a_2), \ldots, \boldsymbol{\nu}_p(a_n)\}} \in \text{ΕΚΠ}_R(a_1, \ldots, a_n)} \tag{5.76}$$

ΑΠΟΔΕΙΞΗ. Εάν οι

$$a_j = u_j \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(a_j)}, \ \ u_j \in R^{\times}, \ \ j \in \{1, \ldots, n\},$$

είναι οι παραστάσεις (5.73) των $a_1, \ldots, a_n$ ως γινομένων πρώτων στοιχείων, τότε $a_j \underset{\text{συν.}}{\sim} \prod_{p \in \mathcal{P}_R} p^{\boldsymbol{\nu}_p(a_j)}$. Έστω c ένα στοιχείο τής R, για το οποίο ισχύει $c \mid a_j$ για κάθε $j \in \{1, \ldots, n\}$. Λαμβάνοντας υπ' όψιν το (ii) τής προτάσεως 5.6.10, για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\boldsymbol{\nu}_p(c) \leq \boldsymbol{\nu}_p(a_j) \Longrightarrow \boldsymbol{\nu}_p(c) \leq \min\left\{\boldsymbol{\nu}_p(a_1), \ldots, \boldsymbol{\nu}_p(a_n)\right\}, \ \forall p \in \mathcal{P}_R.$$

Κατά συνέπειαν, το

$$d := \prod_{p \in \mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a_1), \boldsymbol{\nu}_p(a_2), \ldots, \boldsymbol{\nu}_p(a_n)\}}$$

είναι διαιρέτης τού a_j για κάθε $j \in \{1, \ldots, n\}$ και $d \mid c$. Ως εκ τούτου, το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ και το (5.75) είναι αληθές. Εν συνεχεία, υποθέτουμε ότι το c είναι ένα στοιχείο τής R, για το οποίο ισχύει $a_j \mid c$ για κάθε $j \in \{1, \ldots, n\}$. Λαμβάνοντας εκ νέου υπ' όψιν το (ii) τής προτάσεως 5.6.10, για κάθε $j \in \{1, \ldots, n\}$ έχουμε

$$\boldsymbol{\nu}_p(c) \geq \boldsymbol{\nu}_p(a_j) \Longrightarrow \boldsymbol{\nu}_p(c) \geq \max\left\{\boldsymbol{\nu}_p(a_1), \ldots, \boldsymbol{\nu}_p(a_n)\right\}, \ \forall p \in \mathcal{P}_R.$$

Κατά συνέπειαν, τα a_j είναι διαιρέτες τού

$$t := \prod_{p \in \mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a_1), \boldsymbol{\nu}_p(a_2), \ldots, \boldsymbol{\nu}_p(a_n)\}}$$

για κάθε $j \in \{1, \ldots, n\}$ και $c \mid t$. Ως εκ τούτου, το t είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ και το (5.76) είναι αληθές. □

5.6.12 Πόρισμα. *Εάν ο R είναι μια Π.Μ.Π. και $a, b \in R$, τότε*

$$\boxed{dt \underset{\text{συν.}}{\sim} ab, \ \ \forall d \in \text{ΜΚΔ}_R(a,b) \text{ και } \forall t \in \text{ΕΚΠ}_R(a,b).} \tag{5.77}$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον ένα εκ των a, b είναι $= 0_R$, τότε το (5.77) είναι προφανές. Εάν $a, b \in R \smallsetminus \{0_R\}$, $d \in \text{ΜΚΔ}_R(a,b)$ και $t \in \text{ΕΚΠ}_R(a,b)$, τότε από τις προτάσεις 5.2.12, 5.2.23 και από το θεώρημα 5.6.11 έπεται ότι

$$d \underset{\text{συν.}}{\sim} \prod_{p \in \mathcal{P}_R} p^{\min\{\boldsymbol{\nu}_p(a), \boldsymbol{\nu}_p(b)\}}, \ \ t \underset{\text{συν.}}{\sim} \prod_{p \in \mathcal{P}_R} p^{\max\{\boldsymbol{\nu}_p(a), \boldsymbol{\nu}_p(b)\}}.$$

Χρησιμοποιώντας τήν ισότητα

$$\min\left\{\boldsymbol{\nu}_p(a), \boldsymbol{\nu}_p(b)\right\} + \max\left\{\boldsymbol{\nu}_p(a), \boldsymbol{\nu}_p(b)\right\} = \boldsymbol{\nu}_p(a) + \boldsymbol{\nu}_p(b), \ \forall p \in \mathcal{P}_R,$$

το (i) τής προτάσεως 5.6.10 και όσα προναφέραμε στην 5.2.7, λαμβάνουμε

$$dt \underset{\text{συν.}}{\sim} \left(\prod_{p\in\mathcal{P}_R} p^{\nu_p(a)}\right)\left(\prod_{p\in\mathcal{P}_R} p^{\nu_p(b)}\right) = \prod_{p\in\mathcal{P}_R} p^{\nu_p(a)+\nu_p(b)} = \prod_{p\in\mathcal{P}_R} p^{\nu_p(ab)} \underset{\text{συν.}}{\sim} ab,$$

οπότε το (5.77) είναι αληθές. □

5.6.13 Θεώρημα. *Έστω R μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η R είναι περιοχή με μ.κ.δ. και πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η R είναι Π.Μ.Π, τότε η R είναι περιοχή με μκδ δυνάμει τού θεωρήματος 5.6.11. Ας υποθέσουμε ότι η R δεν πληροί τη συνθήκη των αλυσίδων γνησίων διαιρετών. Τότε υπάρχει μια (άπειρη) ακολουθία $(a_n)_{n\in\mathbb{N}}$ στοιχείων τής R, τέτοια ώστε ο a_{n+1} να είναι *γνήσιος διαιρέτης* τού a_n, για κάθε $n \in \mathbb{N}$, οπότε η ανιούσα αλυσίδα κυρίων ιδεωδών

$$\langle a_1\rangle \subsetneqq \langle a_2\rangle \subsetneqq \cdots \subsetneqq \langle a_n\rangle \subsetneqq \langle a_{n+1}\rangle \subsetneqq \cdots$$

είναι μη στάσιμη. Ιδιαιτέρως, το a_n είναι γνήσιος διαιρέτης τού a_1 για κάθε $n \in \mathbb{N}$, οπότε υπάρχουν *άπειροι* γνήσιοι διαιρέτες τού a_1. Τούτο όμως είναι κάτι το *άτοπο*, διότι το $a_1 \in R \smallsetminus (R^\times \cup \{0_R\})$ διαθέτει ως σύντροφο κάποιον

$$a \underset{\text{συν.}}{\sim} p_1^{\nu_1} p_2^{\nu_2} \cdots p_\ell^{\nu_\ell},$$

όπου τα $p_1, \ldots, p_\ell$ είναι διακεκριμένα πρώτα στοιχεία και $\nu_1, ..., \nu_\ell \in \mathbb{N}_0$, ο οποίος έχει παράγοντες *μονοσημάντως ορισμένους* (με μόνη εξαίρεση την αντικατάστασή τους από ισαρίθμους συντρόφους τους). Ως εκ τούτου, οι μόνοι γνήσιοι διαιρέτες τού a_1 είναι τα στοιχεία τού συνόλου

$$\left\{ p_1^{\mu_1} p_2^{\mu_2} \cdots p_\ell^{\mu_\ell} \;\middle|\; (\mu_1, \ldots, \mu_\ell) \in \left(\prod_{j=1}^{\ell} \{0, 1, ..., \nu_j\}\right) \smallsetminus \{(0, ..., 0), (\nu_1, ..., \nu_\ell)\} \right\}$$

που έχει *πεπερασμένο* πληθικό αριθμό (ίσον με $(\prod_{j=1}^{\ell}(\nu_j + 1)) - 2$). Άρα τελικώς η R οφείλει να πληροί *και* τη συνθήκη των αλυσίδων γνησίων διαιρετών.

(ii)⇒(i) Επειδή η R είναι περιοχή με μ.κ.δ., κάθε ανάγωγο στοιχείο τής R είναι πρώτο (βάσει τής προτάσεως 5.3.6). Επειδή η R πληροί και τη συνθήκη των αλυσίδων γνησίων διαιρετών, είναι, επιπροσθέτως, και περιοχή με παραγοντοποίηση (κατά το θεώρημα 5.6.5). Ως εκ τούτου, η R είναι Π.Μ.Π. βάσει τής ισοδυναμίας (ii)⇔(i) τού θεωρήματος 5.6.3. □

5.7 ΠΟΛΥΩΝΥΜΙΚΟΙ ΔΑΚΤΥΛΙΟΙ ΠΟΥ ΕΙΝΑΙ Π.Μ.Π.

Σε αυτήν την ενότητα θα αποδείξουμε ότι (για μια ακεραία περιοχή R) ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι Π.Μ.Π. εάν και μόνον εάν η ίδια η R είναι Π.Μ.Π. (βλ. θεώρημα 5.7.17).

5.7.1 Ορισμός. Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\},\ n \in \mathbb{N}_0,$$

με τους συντελεστές του $a_0, a_1, \ldots, a_n$ σχετικώς πρώτους εντός τής R (βλ. 5.2.16) καλείται **πρωταρχικό πολυώνυμο (υπεράνω τής** R).

5.7.2 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $p \in R \smallsetminus \{R^{\times} \cup \{0_R\}\}$ ένα πρώτο στοιχείο τής R. Η απεικόνιση*

$$\boxed{\mathfrak{H}_p : R[\mathsf{X}] \longrightarrow (R/\langle p \rangle)[\mathsf{X}],} \tag{5.78}$$

η οριζόμενη μέσω τού τύπου

$$\sum_{j=0}^{n} a_j \mathsf{X}^j = \varphi(\mathsf{X}) \longmapsto \mathfrak{H}_p(\varphi(\mathsf{X})) := \sum_{j=0}^{n} (a_j + \langle p \rangle)\, \mathsf{X}^j,$$

είναι επιμορφισμός από την ακεραία περιοχή $R[\mathsf{X}]$ επί τής ακεραίας περιοχής $(R/\langle p \rangle)[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τον ορισμό των πράξεων προσθέσεως και πολλαπλασιασμού επί τού $R/\langle p \rangle$ τον θεσπισθέντα μέσω τής προτάσεως 2.6.1. (Σημειωτέον ότι η $\mathfrak{H}_p$ είναι ο επιμορφισμός $\theta^{(1)}_{\pi^R_{\langle p \rangle}}$ ο ορισθείς στην άσκηση **3-38**, όπου $\pi^R_{\langle p \rangle} : R \longrightarrow R/\langle p \rangle$ ο φυσικός επιμορφισμός.) Ο πηλικοδακτύλιος $R/\langle p \rangle$ (και, κατ' επέκτασιν, και ο πολυωνυμικός δακτύλιος $(R/\langle p \rangle)[\mathsf{X}]$) είναι ακεραία περιοχή, διότι το $\langle p \rangle$ είναι πρώτο ιδεώδες. (Βλ. 5.3.4 (i), 2.6.4 (i)⇒(ii) και 1.3.9 (ii).) □

5.7.3 Πρόταση. (Λήμμα τού Gauss.) *Έστω R μια Π.Μ.Π. Το γινόμενο $\varphi(\mathsf{X})\psi(\mathsf{X})$ δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$ είναι πρωταρχικό πολυώνυμο εάν και μόνον καθένα εξ αυτών είναι πρωταρχικό πολυώνυμο.*

ΑΠΟΔΕΙΞΗ. Εάν το $\varphi(\mathsf{X})\psi(\mathsf{X})$ είναι πρωταρχικό πολυώνυμο, τότε *κάθε* κοινός διαιρέτης των συντελεστών τού $\varphi(\mathsf{X})$ διαιρεί καθέναν εκ των συντελεστών τού $\varphi(\mathsf{X})\psi(\mathsf{X})$, οπότε είναι ένα αντιστρέψιμο στοιχείο τής R. Άρα το $\varphi(\mathsf{X})$ είναι ένα πρωταρχικό πολυώνυμο. Μέσω τής ίδιας επιχειρηματολογίας δείχνουμε ότι το $\psi(\mathsf{X})$ είναι ωσαύτως πρωταρχικό.

Αντιστρόφως τώρα· έστω ότι τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι πρωταρχικά πολυώνυμα. Ας υποθέσουμε ότι το γινόμενό τους $\varphi(\mathsf{X})\psi(\mathsf{X})$ *δεν* είναι πρωταρχικό πολυώνυμο. Θεωρούμε έναν μέγιστο κοινό διαιρέτη d των συντελεστών τού $\varphi(\mathsf{X})\psi(\mathsf{X})$ και ένα πρώτο (= ανάγωγο) στοιχείο $p \in R \smallsetminus \{R^\times \cup \{0_R\}\}$ τής R που διαιρεί τον d. (Προφανώς, $d \notin R^\times \cup \{0_R\}$.) Η εικόνα τού $\varphi(\mathsf{X})\psi(\mathsf{X})$ μέσω τού ομομορφισμού (5.78) είναι η εξής:

$$\mathfrak{H}_p(\varphi(\mathsf{X}))\mathfrak{H}_p(\psi(\mathsf{X})) = \mathfrak{H}_p(\varphi(\mathsf{X})\psi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]} = \langle p\rangle\,[\mathsf{X}],$$

καθότι το p διαιρεί όλους τους συντελεστές τού $\varphi(\mathsf{X})\psi(\mathsf{X})$, οπότε καθένας εξ αυτών ανήκει στο κύριο ιδεώδες $\langle p\rangle$. Επειδή ο πηλικοδακτύλιος $R/\langle p\rangle$ είναι ακεραία περιοχή, έχουμε *είτε* $\mathfrak{H}_p(\varphi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]}$ είτε $\mathfrak{H}_p(\psi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]}$, δηλαδή *είτε* το p είναι κοινός διαιρέτης όλων των συντελεστών τού $\varphi(\mathsf{X})$ *είτε* το p είναι κοινός διαιρέτης όλων των συντελεστών τού $\psi(\mathsf{X})$. Στην πρώτη περίπτωση το p οφείλει να διαιρεί *κάθε* μέγιστο κοινό διαιρέτη των συντελεστών τού $\varphi(\mathsf{X})$, οπότε $p \mid 1_R$ (διότι το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό), πράγμα *αδύνατο* (καθόσον $p \notin R^\times$). Κατ' αναλογίαν, δείχνουμε ότι *και* στη δεύτερη περίπτωση καταλήγουμε σε άτοπο (διότι *και* το $\psi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό). □

5.7.4 Λήμμα. *Έστω R μια Π.Μ.Π. Για οιοδήποτε $\varphi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$ ισχύουν τα ακόλουθα:*

(i) *Υπάρχει κάποιο στοιχείο $c \in \mathbf{Fr}(R)$, καθώς και κάποιο $\widetilde{\varphi}(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, πρωταρχικό υπεράνω τής R, ούτως ώστε να ισχύει η ισότητα*

$$\varphi(\mathsf{X}) = c\,\widetilde{\varphi}(\mathsf{X}). \tag{5.79}$$

(ii) *Η έκφραση (5.79) τού $\varphi(\mathsf{X})$ είναι «κατ' ουσίαν μοναδική» υπό την εξής έννοια: Εάν υπάρχει κάποιο άλλο στοιχείο $c' \in \mathbf{Fr}(R)$, καθώς και κάποιο πολυώνυμο $\widetilde{\varphi}'(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, πρωταρχικό υπεράνω τής R, ούτως ώστε να ισχύει η ισότητα $\varphi(\mathsf{X}) = c'\,\widetilde{\varphi}'(\mathsf{X})$, τότε $\exists u \in R^\times : c' = uc$, με $\widetilde{\varphi}'(\mathsf{X}) = u^{-1}\widetilde{\varphi}(\mathsf{X})$ όταν $\varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}$.*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν πολυώνυμο $\varphi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$. Γράφοντας το $\varphi(\mathsf{X})$ αναλυτικώς υπό τη μορφή

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} \frac{a_j}{b_j}\mathsf{X}^j,\ n \in \mathbb{N}_0,$$

όπου $(a_j, b_j) \in R \times (R\smallsetminus\{0_R\}), \forall j \in \{0, \ldots, n\}$, και θέτοντας $b := \prod_{j=0}^{n} b_j$ λαμβάνουμε

$$\varphi(\mathsf{X}) = b^{-1}\psi(\mathsf{X}), \text{ όπου } \psi(\mathsf{X}) := \sum_{j=0}^{n}\left(a_j\left(\prod_{k\in\{0,\ldots,n\}\smallsetminus\{j\}} b_k\right)\right)\mathsf{X}^j \in R[\mathsf{X}].$$

Εν συνεχεία, θεωρώντας τυχόντα $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \psi(\mathsf{X})\})$ και θέτοντας

$$\widetilde{\varphi}(\mathsf{X}) := \begin{cases} 1_R, & \text{όταν } \varphi(\mathsf{X}) = 0_{\mathbf{Fr}(R)[\mathsf{X}]}, \\ d^{-1}\psi(\mathsf{X}), & \text{όταν } \varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}, \end{cases}$$

παρατηρούμε ότι το $\widetilde{\varphi}(\mathsf{X})$ είναι πρωταρχικό πολυώνυμο υπεράνω τής R. Επειδή $\varphi(\mathsf{X}) = db^{-1}\,\widetilde{\varphi}(\mathsf{X})$ αρκεί να θέσουμε $c := db^{-1}$.

(ii) Εξ υποθέσεως,

$$\varphi(\mathsf{X}) = c\,\widetilde{\varphi}(\mathsf{X}) = c'\,\widetilde{\varphi}'(\mathsf{X}).$$

Εκφράζοντας τα c, c' υπό τη μορφή κλασμάτων:

$$c = \frac{r_1}{r_2},\ c' = \frac{r_1'}{r_2'},\ r_1, r_1' \in R,\ r_2, r_2' \in R\smallsetminus\{0_R\},$$

και λαμβάνοντας υπ' όψιν ότι $r_2 r_2' \neq 0_R$, καταλήγουμε στην ισότητα

$$r_1 r_2' \widetilde{\varphi}(\mathsf{X}) = r_1' r_2 \widetilde{\varphi}'(\mathsf{X}). \tag{5.80}$$

Επειδή τα $\widetilde{\varphi}(\mathsf{X}), \widetilde{\varphi}'(\mathsf{X})$ είναι πρωταρχικά πολυώνυμα, έχουμε

$$\begin{aligned} r_1 r_2' &\in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } r_1 r_2' \widetilde{\varphi}(\mathsf{X})\}), \\ r_1' r_2 &\in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } r_1' r_2 \widetilde{\varphi}'(\mathsf{X})\}), \end{aligned}$$

(βλ. 5.2.35 (iv)), οπότε η (5.80), σε συνδυασμό με το (ii) τής προτάσεως 5.2.12, δίδει $r_1 r_2' \underset{\text{συν.}}{\sim} r_1' r_2$. Άρα υπάρχει κάποιο $u \in R^\times$, τέτοιο ώστε να ισχύει

$$r_1' r_2 = u r_1 r_2' \Rightarrow c' = uc$$

(βλ. πόρισμα 5.2.5). Όταν $\varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}$, λαμβάνουμε $\widetilde{\varphi}'(\mathsf{X}) = u^{-1}\widetilde{\varphi}(\mathsf{X})$ (καθόσον $c \neq 0_R$ και $c' \neq 0_R$). □

5.7.5 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι ένα πολυώνυμο θετικού βαθμού και εάν υπάρχουν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, τότε*

$$\exists c \in \mathbf{Fr}(R)\smallsetminus\{0_{\mathbf{Fr}(R)}\} : c\,\varphi_1(\mathsf{X}) \in R[\mathsf{X}] \text{ και } c^{-1}\,\varphi_2(\mathsf{X}) \in R[\mathsf{X}].$$

ΑΠΟΔΕΙΞΗ. Έστω $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \varphi(\mathsf{X})\})$. Προφανώς, $d \neq 0_R$, και το πολυώνυμο $\overline{\varphi}(\mathsf{X}) := d^{-1}\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Σύμφωνα με το (i) τού λήμματος 5.7.4 υπάρχουν $c_1, c_2 \in \mathbf{Fr}(R)$, καθώς και κάποια πολυώνυμα $\widetilde{\varphi}_1(\mathsf{X}), \widetilde{\varphi}_2(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, πρωταρχικά υπεράνω τής R, ούτως ώστε να ισχύουν οι ισότητες

$$\varphi_1(\mathsf{X}) = c_1\, \widetilde{\varphi}_1(\mathsf{X}) \ \text{ και } \ \varphi_2(\mathsf{X}) = c_2\, \widetilde{\varphi}_2(\mathsf{X}).$$

Το γινόμενο $\widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ των πρωταρχικών πολυωνύμων $\widetilde{\varphi}_1(\mathsf{X})$ και $\widetilde{\varphi}_2(\mathsf{X})$ είναι πρωταρχικό (βλ. πρόταση 5.7.3). Επομένως, επειδή αμφότερα τα $\overline{\varphi}(\mathsf{X})$ και $\widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ είναι πρωταρχικά, και

$$d\,\overline{\varphi}(\mathsf{X}) = \varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) = (c_1c_2)\, \widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X}),$$

εφαρμόζοντας το (ii) τού λήμματος 5.7.4 (με τα $d, \overline{\varphi}(\mathsf{X}), c_1c_2, \widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ στη θέση των εκεί παρατεθέντων $c\,, \widetilde{\varphi}(\mathsf{X}), c'$ και $\widetilde{\varphi}'(\mathsf{X})$) εξασφαλίζουμε την ύπαρξη ενός στοιχείου $u \in R^{\times}$, τέτοιου ώστε να ισχύει $c_1c_2 = ud$. Θέτοντας $c := c_2$ λαμβάνουμε $c\,\varphi_1(\mathsf{X}) = c_1c_2\,\widetilde{\varphi}_1(\mathsf{X}) \in R[\mathsf{X}]$ και $c^{-1}\,\varphi_2(\mathsf{X}) = \widetilde{\varphi}_2(\mathsf{X}) \in R[\mathsf{X}]$. $\square$

5.7.6 Σημείωση. (i) Έστω R μια ακεραία περιοχή. Προφανώς, ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι ανάγωγο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$ εάν και μόνον εάν

(a) δεν είναι σταθερό πολυώνυμο τής μορφής $\varphi(\mathsf{X}) = r, r \in R^{\times} \cup \{0_R\}$, και

(b) γραφόμενο ως γινόμενο $\varphi(\mathsf{X}) = \psi(\mathsf{X})\chi(\mathsf{X}), \psi(\mathsf{X}), \chi(\mathsf{X}) \in R\,[\mathsf{X}]$, ισχύει

$$\text{είτε } \ \psi(\mathsf{X}) = a \in R^{\times} \ \text{ είτε } \ \chi(\mathsf{X}) = b \in R^{\times}.$$

(Βλ. 5.3.2 και 1.3.9 (iii).) Εν τοιαύτη περιπτώσει, για λόγους συντομίας, λέμε ότι το $\varphi(\mathsf{X})$ είναι **ανάγωγο υπεράνω τής** R.

(ii) Εάν το K είναι τυχόν *σώμα*, τότε ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ είναι ανάγωγο υπεράνω τού K εάν και μόνον εάν

(a′) δεν είναι σταθερό πολυώνυμο (ήτοι $\deg(\varphi(\mathsf{X})) \geq 1$) και

(b′) δεν μπορεί να εκφρασθεί ως γινόμενο $\varphi(\mathsf{X}) = \psi(\mathsf{X})\chi(\mathsf{X})$ δύο πολυωνύμων $\psi(\mathsf{X}), \chi(\mathsf{X}) \in K\,[\mathsf{X}]$, με

$$1 \leq \deg(\psi(\mathsf{X})) < \deg(\varphi(\mathsf{X})) \ \text{ και } \ 1 \leq \deg(\chi(\mathsf{X})) < \deg(\varphi(\mathsf{X})),$$

αφού (σύμφωνα με το (i) τού πορίσματος 1.3.10)

$$K\,[\mathsf{X}]^{\times} = K^{\times} = K \smallsetminus \{0_K\} = \{\,\varphi\,(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(\varphi(\mathsf{X})) = 0\}\,.$$

5.7.7 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ θετικού βαθμού είναι ανάγωγο υπεράνω τής R, τότε είναι ανάγωγο και υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ ένα πολυώνυμο θετικού βαθμού, ανάγωγο υπεράνω τής R. Εάν το $\varphi(\mathsf{X})$ δεν ήταν ανάγωγο υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R, τότε θα υπήρχαν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$ θετικού βαθμού με $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, καθώς κάποιο στοιχείο $c \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\}$, τέτοιο ώστε $c\,\varphi_1(\mathsf{X}) \in R[\mathsf{X}]$ και $c^{-1}\,\varphi_2(\mathsf{X}) \in R[\mathsf{X}]$ (βλ. λήμμα 5.7.5). Εξ αυτού θα προέκυπτε ότι

$$\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) = (c\,\varphi_1(\mathsf{X}))\,(c^{-1}\,\varphi_2(\mathsf{X}))$$

με $\deg(c\,\varphi_1(\mathsf{X})) \geq 1$ και $\deg(c^{-1}\,\varphi_2(\mathsf{X})) \geq 1$, κάτι το οποίο θα αντέκειτο προς την αρχική μας υπόθεση. Άρα το $\varphi(\mathsf{X})$ είναι κατ' ανάγκην ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$. $\square$

5.7.8 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $r \in R$. Για οιοδήποτε*

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in R[\mathsf{X}] \ (n \in \mathbb{N}_0)$$

τα ακόλουθα είναι ισοδύναμα:

(i) $r \mid a_j,\ \forall j \in \{0, \ldots, n\}$.

(ii) *Το r (θεωρούμενο ως σταθερό πολυώνυμο) διαιρεί το $\varphi(\mathsf{X})$ εντός τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ υποθέσεως, $\exists b_j \in R : a_j = rb_j$ για κάθε $j \in \{0, \ldots, n\}$. Επομένως,

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} (rb_j)\,\mathsf{X}^j = r\left(\sum_{j=0}^{n} b_j \mathsf{X}^j\right) \Rightarrow r \mid \varphi(\mathsf{X}).$$

(ii)⇒(i) Εάν $r \mid \varphi(\mathsf{X})$ (εντός τής $R[\mathsf{X}]$), τότε *είτε* $r = 0_R\ (= 0_{R[\mathsf{X}]})$, οπότε έχουμε $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ (και το (i) είναι προφανές) *είτε*

$$r \neq 0_R \ \text{ και } \ \exists \psi(\mathsf{X}) \in R[\mathsf{X}] : \varphi(\mathsf{X}) = r\psi(\mathsf{X}).$$

Εν τοιαύτη περιπτώσει, $\psi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ όταν $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$, ενώ όταν $\varphi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$ και $\deg(\varphi(\mathsf{X})) = n$, έχουμε $\deg(\psi(\mathsf{X})) = n$ (βλ. 1.3.9 (i)) και υπάρχουν $c_0, \ldots, c_n \in R$ (με $c_n \neq 0_R$), τέτοια ώστε

$$\psi(\mathsf{X}) = \sum_{j=0}^{n} c_j \mathsf{X}^j \Rightarrow \varphi(\mathsf{X}) = r\left(\sum_{j=0}^{n} c_j \mathsf{X}^j\right) = \sum_{j=0}^{n} (rc_j)\,\mathsf{X}^j,$$

οπότε $a_j = rc_j$ για κάθε $j \in \{0, \ldots, n\}$. □

5.7.9 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τού R και ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$, τότε είναι ανάγωγο και υπεράνω τής R.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ ένα πολυώνυμο πρωταρχικό υπεράνω τού R και ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$. Τότε αυτό είναι προφανώς μη μηδενικό· επιπροσθέτως, έχει θετικό βαθμό (διότι κάθε σταθερό, μη μηδενικό, πρωταρχικό πολυώνυμο ανήκον στην ακεραία περιοχή $R[\mathsf{X}]$ ισούται με ένα αντιστρέψιμο στοιχείο τού R). Ας υποθέσουμε ότι $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, για κάποια πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in R[\mathsf{X}]$. Αυτή η ισότητα μπορεί να ιδωθεί και ως μια παραγοντοποίηση τού $\varphi(\mathsf{X})$ *εντός τού* $\mathbf{Fr}(R)[\mathsf{X}]$. Επομένως, τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ οφείλει να είναι σταθερό, μη μηδενικό. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $\varphi_1(\mathsf{X}) = c \in R \smallsetminus \{0_R\}$. Σύμφωνα με το λήμμα 5.7.8 το c διαιρεί όλους τους συντελεστές τού $\varphi(\mathsf{X})$. Αυτό σημαίνει ότι $c \mid 1_{\mathbf{Fr}(R)}$ $(= 1_R)$, διότι το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό υπεράνω τού $\mathbf{Fr}(R)$. Επομένως, $c \in R^\times$ ή, ισοδυνάμως, $\varphi_1(\mathsf{X}) \in R[\mathsf{X}]^\times$, οπότε το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τής R. □

5.7.10 Σημείωση. Η «πρωταρχικότητα» τού $\varphi(\mathsf{X})$ δεν μπορεί να παραλειφθεί από τις προϋποθέσεις τού λήμματος 5.7.9. Επί παραδείγματι, το $4\mathsf{X} + 6$ είναι ανάγωγο υπεράνω τού $\mathbb{Q}$ αλλά δεν είναι ανάγωγο υπεράνω τού $\mathbb{Z}$, διότι $4\mathsf{X} + 6 = 2(2\mathsf{X} + 3)$, όπου $2 \notin \{\pm 1\} = \mathbb{Z}^\times$ και $2\mathsf{X} + 3 \notin \mathbb{Z}^\times$.

5.7.11 Λήμμα. *Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ θετικού βαθμού που είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$, είναι πρώτο στοιχείο και τού $\mathbf{Fr}(R)[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X})$ ένα πολυώνυμο θετικού βαθμού που είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$. Τότε το $\varphi(\mathsf{X})$ είναι ανάγωγο στοιχείο τής $R[\mathsf{X}]$ (ήτοι ανάγωγο υπεράνω τής R) επί τη βάσει τού (iii) τής προτάσεως 5.3.4. Σύμφωνα με το λήμμα 5.7.7, αυτό είναι ανάγωγο και υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R. Τέλος, επειδή ο πολυωνυμικός δακτύλιος $\mathbf{Fr}(R)[\mathsf{X}]$ είναι Π.Κ.Ι. (βλ. 5.4.24 (iii)⇒(ii)), το $\varphi(\mathsf{X})$ οφείλει να είναι πρώτο στοιχείο *και* τού $\mathbf{Fr}(R)[\mathsf{X}]$ (βλ. 5.3.4 (iv)). □

5.7.12 Λήμμα. *Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ που είναι πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$ και πρωταρχικό υπεράνω τού R, είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ εντός τού $R[\mathsf{X}]$ για κάποια πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$, τότε είτε $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})$ είτε $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ *εντός* *τού* $\mathbf{Fr}(R)[\mathsf{X}]$. Ας υποθέσουμε ότι

$$\exists \psi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}] : \varphi_1(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}). \tag{5.81}$$

Έστω $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \varphi(\mathsf{X})\})$. Προφανώς, $d \neq 0_R$, και το πολυώνυμο $\overline{\varphi}(\mathsf{X}) := d^{-1}\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Σύμφωνα με το (i) τού λήμματος 5.7.4 υπάρχουν $c_1, c \in \mathbf{Fr}(R)$, καθώς και κάποια πολυώνυμα $\widetilde{\varphi}_1(\mathsf{X}), \widetilde{\psi}(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, πρωταρχικά υπεράνω τής R, ούτως ώστε να ισχύουν οι ισότητες

$$\varphi_1(\mathsf{X}) = c_1\,\widetilde{\varphi}_1(\mathsf{X}) \;\text{ και }\; \psi(\mathsf{X}) = c\,\widetilde{\psi}(\mathsf{X}).$$

Η (5.81) δίδει $c_1\,\widetilde{\varphi}_1(\mathsf{X}) = c\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X})$. Επειδή (κατά την πρόταση 5.7.3) το $\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X})$ είναι πρωταρχικό υπεράνω τής R, το (ii) τού λήμματος 5.7.4 μας πληροφορεί ότι $\exists u \in R^{\times} : c = uc_1$. Εάν $\varphi_1(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε (προφανώς) $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})$ *εντός τής* $R[\mathsf{X}]$. Εάν $\varphi_1(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, τότε $c_1 \neq 0_R$ και

$$\widetilde{\varphi}_1(\mathsf{X}) = u\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X}) \Rightarrow \varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X}) \;\; (\text{εντός τής } R[\mathsf{X}]).$$

(Εάν $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ εντός τού $\mathbf{Fr}(R)[\mathsf{X}]$, τότε η απόδειξη τού ότι ισχύει $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ *και* εντός τής $R[\mathsf{X}]$ είναι πανομοιότυπη.) Άρα το $\varphi(\mathsf{X})$ είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$. □

5.7.13 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $p \in R$. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Το p είναι ένα πρώτο στοιχείο τής R.*

(ii) *Το σταθερό πολυώνυμο $\varphi(\mathsf{X}) := p$ είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ ορισμού, $p \in R \smallsetminus (R^{\times} \cup \{0_R\})$. Επειδή $R[\mathsf{X}]^{\times} = R^{\times}$ και $0_{R[\mathsf{X}]} = 0_R$, έχουμε

$$\varphi(\mathsf{X}) := p \in R[\mathsf{X}] \smallsetminus (R[\mathsf{X}]^{\times} \cup \{0_{R[\mathsf{X}]}\}).$$

Έστω ότι $\varphi(\mathsf{X}) := p \mid \psi(\mathsf{X})\chi(\mathsf{X})$, για κάποια πολυώνυμα

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],\; \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}].$$

Υποθέτοντας ότι $p \nmid \psi(\mathsf{X})$ και $p \nmid \chi(\mathsf{X})$, το λήμμα 5.7.8 μας πληροφορεί ότι

$$[\exists i_0 \in \{0, \ldots, n\} : p \nmid a_{i_0}] \;\text{ και }\; [\exists j_0 \in \{0, \ldots, m\} : p \nmid b_{j_0}].$$

Θέτοντας $k := \min\{i \in \{0, \ldots, n\} : p \nmid a_i\}$ και $l := \min\{j \in \{0, \ldots, m\} : p \nmid b_j\}$, παρατηρούμε ότι

$$p \mid a_i b_j \text{ όταν } i + j = k + l \text{ και είτε } i < k \text{ είτε } j < l,$$

αλλά $p \nmid a_k b_l$, οπότε $p \nmid \sum_{i+j=k+l} a_i b_j$, δηλαδή το p δεν διαιρεί τον $(k+l)$-στό συντελεστή τού πολυωνύμου $\psi(\mathsf{X})\chi(\mathsf{X})$, κάτι το οποίο είναι αδύνατο (εκ νέου λόγω τού λήμματος 5.7.8). Άρα είτε $p \mid \psi(\mathsf{X})$ είτε $p \mid \chi(\mathsf{X})$ και, ως εκ τούτου, το $\varphi(\mathsf{X}) := p$ είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.

(ii)⇒(i) Τούτο είναι προφανές. □

5.7.14 Πρόταση. *Ο δακτύλιος $R[\mathsf{X}]$ είναι Π.Μ.Π. για κάθε Π.Μ.Π. R.*

Απόδειξη. Έστω R τυχούσα Π.Μ.Π. και έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus (R[\mathsf{X}]^{\times} \cup \{0_{R[\mathsf{X}]}\})$. Αρκεί να αποδείξουμε ότι το $\varphi(\mathsf{X})$ διαθέτει κάποιο συντροφικό του πολυώνυμο παριστώμενο ως γινόμενο πεπερασμένου πλήθους πρώτων στοιχείων τής ακεραίας περιοχής $R[\mathsf{X}]$ (βλ. 5.6.3 (iii)⇒(i)). Το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή $\varphi(\mathsf{X}) = d\overline{\varphi}(\mathsf{X})$, όπου $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \varphi(\mathsf{X})\})$ και $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Προφανώς, $d \neq 0_R$. Επιπροσθέτως, είναι αδύνατον να ισχύει $d \in R^{\times}$ και *ταυτοχρόνως* $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]^{\times}$ $(= R^{\times})$, διότι $\varphi(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$. Άρα υπάρχουν τρία ενδεχόμενα:

Περίπτωση πρώτη. $d \notin R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]^{\times}$ $(= R^{\times})$.

Περίπτωση δεύτερη. $d \in R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$.

Περίπτωση τρίτη. $d \notin R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$.

Στην πρώτη περίπτωση έχουμε $\overline{\varphi}(\mathsf{X}) = w$, για κάποιο $w \in R^{\times}$, και το d γράφεται υπό τη μορφή $d = uq_1 \cdots q_k$, όπου $w \in R^{\times}$, $k \in \mathbb{N}$, και τα $q_1, \ldots, q_k$ είναι πρώτα στοιχεία τής R (διότι η R είναι Π.Μ.Π.). Άρα

$$\varphi(\mathsf{X}) = d\overline{\varphi}(\mathsf{X}) = (uw)q_1 \cdots q_k,$$

όπου τα $q_1, \ldots, q_k$ (θεωρούμενα ως σταθερά πολυώνυμα) είναι πρώτα στοιχεία τής ακεραίας περιοχής $R[\mathsf{X}]$ (βλ. 5.7.13 (i)⇒(ii)).

Εν συνεχεία, θα εξετάσουμε τη δεύτερη και την τρίτη περίπτωση. Εάν το $\overline{\varphi}(\mathsf{X})$ είναι σταθερό, δηλαδή εάν $\overline{\varphi}(\mathsf{X}) = r$ για κάποιο $r \in R \smallsetminus (R^{\times} \cup \{0_R\})$, τότε γράφοντας το r υπό τη μορφή $r = zt_1 \cdots t_l$, όπου $z \in R^{\times}$, $l \in \mathbb{N}$, και τα $t_1, \ldots, t_k$ πρώτα στοιχεία τής R, λαμβάνουμε

$$\varphi(\mathsf{X}) = \begin{cases} (dz)\, t_1 \cdots t_l, & \text{όταν } d \in R^{\times}, \\ (uz)q_1 \cdots q_k t_1 \cdots t_l, & \text{όταν } d = uq_1 \cdots q_k \text{ (όπως στην 1η περ.)} \end{cases}$$

Εάν $\deg(\overline{\varphi}(\mathsf{X})) \geq 1$, τότε το $\overline{\varphi}(\mathsf{X})$, ιδωμένο ως στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$, παριστάται ως γινόμενο

$$\overline{\varphi}(\mathsf{X}) = \lambda\psi_1(\mathsf{X})\cdots\psi_m(\mathsf{X}),\ \lambda \in R^\times,\ m \in \mathbb{N}, \tag{5.82}$$

μιας σταθεράς και m πρώτων στοιχείων $\psi_1(\mathsf{X}),\ldots,\psi_m(\mathsf{X})$ τού $\mathbf{Fr}(R)[\mathsf{X}]$ (καθόσον ο $\mathbf{Fr}(R)[\mathsf{X}]$ είναι Π.Μ.Π., βλ. 5.4.24 (iii)⇒(ii), πόρισμα 5.6.8 και 5.6.3 (i)⇒(iii)). Σύμφωνα με το (i) τού λήμματος 5.7.4 υπάρχουν πολυώνυμα $\chi_i(\mathsf{X}) \in R[\mathsf{X}]$, πρωταρχικά υπεράνω τού R, και

$$\exists (a_i, b_i) \in R \times (R \smallsetminus \{0_R\}) : \psi_i(\mathsf{X}) = \frac{a_i}{b_i}\chi_i(\mathsf{X}),$$

για κάθε $i \in \{1,\ldots,m\}$. Εντός τής ακεραίας περιοχής $R[\mathsf{X}]$ ισχύει η ισότητα

$$b\,\overline{\varphi}(\mathsf{X}) = (\lambda a)\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}),$$

όπου τόσον το $\overline{\varphi}(\mathsf{X})$ (εκ κατασκευής) όσον και το γινόμενο $\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X})$ (λόγω τής προτάσεως 5.7.3) είναι πρωταρχικά πολυώνυμα υπεράνω τού R. Το (ii) τού λήμματος 5.7.4 μας πληροφορεί ότι $\exists \xi \in R^\times : \lambda a = \xi b$. Επομένως η (5.82) δίδει

$$b \neq 0_R \Longrightarrow \overline{\varphi}(\mathsf{X}) = \xi\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}).$$

Σημειωτέον ότι για κάθε δείκτη $i \in \{1,\ldots,m\}$ έχουμε

$$\psi_i(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]} \Rightarrow a_i \neq 0_R \Rightarrow \frac{a_i}{b_i} \in \mathbf{Fr}(R)\smallsetminus\{0_{\mathbf{Fr}(R)}\}\ (= \mathbf{Fr}(R)^\times),$$

οπότε τα $\psi_i(\mathsf{X})$ και $\chi_i(\mathsf{X})$ είναι συντροφικά εντός τού $\mathbf{Fr}(R)[\mathsf{X}]$. Επειδή το $\psi_i(\mathsf{X})$ είναι πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$, το $\chi_i(\mathsf{X})$ είναι ωσαύτως πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$ (βλ. 5.3.4 (v)) και, κατ' επέκτασιν, *πρώτο στοιχείο τής ακεραίας περιοχής* $R[\mathsf{X}]$ (δυνάμει τού λήμματος 5.7.12). Τελικώς λοιπόν η

$$\varphi(\mathsf{X}) = \begin{cases} (d\xi)\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}), & \text{όταν } d \in R^\times, \\ (u\xi)q_1\cdots q_k\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}), & \text{όταν } d = uq_1\cdots q_k \\ & \text{(όπως στην 1η περ.)} \end{cases}$$

είναι η ζητούμενη παραγοντοποίηση. □

5.7.15 Σημείωση. (i) Σύμφωνα με την πρόταση 5.7.14, ο πολυωνυμικός δακτύλιος $\mathbb{Z}[\mathsf{X}]$ είναι Π.Μ.Π. Ωστόσο, όπως γνωρίζουμε από την πρόταση 5.4.24, αυτός δεν είναι Π.Κ.Ι.

(ii) Πηλικοδακτύλιοι δομούμενοι μέσω περιοχών μονοσήμαντης παραγοντοποιήσεως δεν είναι απαραιτήτως Π.Μ.Π. Επί παραδείγματι, έχουμε

$$\mathbb{Z}[\mathsf{X}]/\left\langle \mathsf{X}^2 + 3 \right\rangle \cong \mathbb{Z}[\sqrt{-3}],$$

όπου η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-3}]$ δεν είναι Π.Μ.Π.

5.7.16 Πόρισμα. *Ο πολυωνυμικός δακτύλιος* $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ *είναι Π.Μ.Π. για κάθε Π.Μ.Π.* R *και για κάθε* $n \in \mathbb{N}$.

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί η πρόταση 5.7.14 και μαθηματική επαγωγή ως προς τον n. □

5.7.17 Θεώρημα. *Έστω* R *μια ακεραία περιοχή. Οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η* R *είναι Π.Μ.Π.*

(ii) *Η ακεραία περιοχή* $R[\mathsf{X}]$ *είναι Π.Μ.Π.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Βλ. πρόταση 5.7.14.

(ii)⇒(i) Εάν η ακεραία περιοχή $R[\mathsf{X}]$ είναι Π.Μ.Π. και $a \in R \smallsetminus (R^{\times} \cup \{0_R\})$, τότε, θεωρώντας τό a ως ένα σταθερό πολυώνυμο ανήκον στην $R[\mathsf{X}]$, το γράφουμε υπό τη μορφή

$$a = u\gamma_1(\mathsf{X}) \cdots \gamma_k(\mathsf{X}),\ k \in \mathbb{N},\ u \in R[\mathsf{X}]^{\times} = R^{\times},$$

όπου τα $\gamma_1(\mathsf{X}), \ldots, \gamma_k(\mathsf{X})$ είναι ανάγωγα (και, ως εκ τούτου, πρώτα) στοιχεία τής $R[\mathsf{X}]$. Επειδή ο βαθμός τού αριστερού μέλος τής ανωτέρω ισότητας οφείλει να ισούται με τον βαθμό τού δεξιού της μέλους, λαμβάνουμε

$$\deg(\gamma_1(\mathsf{X})) = \cdots = \deg(\gamma_k(\mathsf{X})) = 0$$

οπότε καθένα εκ των $\gamma_1(\mathsf{X}), \ldots, \gamma_k(\mathsf{X})$ είναι ένα μη μηδενικό σταθερό πολυώνυμο, ήτοι ένα πρώτο στοιχείο τής R (βλ. 5.7.13 (ii)⇒(i)). Κατά συνέπειαν, και η ίδια η R είναι Π.Μ.Π. (βλ. 5.6.3 (iii)⇒(i)). □

5.7.18 Πόρισμα. *Έστω* R *μια ακεραία περιοχή. Οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η* R *είναι Π.Μ.Π.*

(ii) *Η ακεραία περιοχή* $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ *είναι Π.Μ.Π. για κάθε* $n \in \mathbb{N}$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 5.7.17 και το πόρισμα 5.7.16. □

► **Κριτήριο αναγωγιμότητας τού Eisenstein**. Κάνοντας χρήση τού επιμορφισμού (5.78) και τού λήμματος 5.7.5 είναι δυνατόν να αποδειχθεί το ακόλουθο λίαν σημαντικό θεώρημα:

5.7.19 Θεώρημα. (Eisenstein, 1850) *Έστω* R *μια Π.Μ.Π. και έστω*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]$$

ένα πολυώνυμο βαθμού $n \geq 1$. Εάν υπάρχει ένα πρώτο στοιχείο p τής R, τέτοιο ώστε

(i) $p \mid a_i, \ \forall i \in \{0, \ldots, n-1\}$,

(ii) $p \nmid a_n$ *και*

(iii) $p^2 \nmid a_0$,

τότε το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$ (και ανάγωγο υπεράνω τής R όταν είναι πρωταρχικό υπεράνω τής R).

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ για κάποια πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$ *θετικού βαθμού*. Τότε

$$\varphi(\mathsf{X}) = \psi_1(\mathsf{X})\psi_2(\mathsf{X}), \ \psi_1(\mathsf{X}) = t\,\varphi_1(\mathsf{X}) \in R[\mathsf{X}], \psi_2(\mathsf{X}) = t^{-1}\,\varphi_2(\mathsf{X}) \in R[\mathsf{X}],$$

για κάποιο κατάλληλο $t \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\}$ (δυνάμει τού λήμματος 5.7.5). Σημειωτέον ότι $\deg(\psi_1(\mathsf{X})) = \deg(\varphi_1(\mathsf{X}))$ και $\deg(\psi_2(\mathsf{X})) = \deg(\varphi_2(\mathsf{X}))$. Λόγω των προϋποτεθεισών συνθηκών (i) και (ii) η εφαρμογή τού επιμορφισμού (5.78) στο $\varphi(\mathsf{X})$ δίδει

$$\begin{aligned} \mathfrak{H}_p(\psi_1(\mathsf{X}))\mathfrak{H}_p(\psi_2(\mathsf{X})) &= \mathfrak{H}_p(\psi_1(\mathsf{X})\psi_2(\mathsf{X})) \\ &= \mathfrak{H}_p(\varphi(\mathsf{X})) = (a_n + \langle p \rangle)\,\mathsf{X}^n \end{aligned}$$

και οι εικόνες των $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ μέσω αυτού οφείλουν να εκφράζονται ως εξής:

$$\mathfrak{H}_p(\psi_1(\mathsf{X})) = (b_m + \langle p \rangle)\,\mathsf{X}^m, \ \mathfrak{H}_p(\psi_2(\mathsf{X})) = (c_{n-m} + \langle p \rangle)\,\mathsf{X}^{n-m}, \tag{5.83}$$

για κάποιον φυσικό αριθμό m με $0 < m < n$ και $b_m, c_{n-m} \in R$ (διότι ο πολυωνυμικός δακτύλιος $(R/\langle p \rangle)[\mathsf{X}]$) είναι ακεραία περιοχή, πρβλ. 1.3.9 (i)). Επιπροσθέτως, τα $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ είναι κατ' ανάγκην τής μορφής

$$\psi_1(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j, \ \psi_2(\mathsf{X}) = \sum_{k=0}^{n-m} c_k \mathsf{X}^k,$$

όπου $b_0, \ldots, b_{m-1}, c_0, \ldots, c_{n-m-1} \in R$ με $p \mid b_0$ και $p \mid c_0$ (λόγω των (5.83)!). Επομένως, $p^2 \mid b_0 c_0 = a_0$, κάτι που αντίκειται προς τη συνθήκη (iii). Κατά συνέπειαν, τουλάχιστον ένα εκ των (εκ κατασκευής μη μηδενικών) $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ είναι σταθερό και, ως εκ τούτου, τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ είναι σταθερό. Αυτό σημαίνει ότι το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$ (και ανάγωγο υπεράνω τής R όταν είναι πρωταρχικό υπεράνω τής R επί τη βάσει τού λήμματος 5.7.9). □

5.7.20 Παράδειγμα. Έστω $\varphi(\mathsf{X}) := 3\mathsf{X}^5 + 15\mathsf{X}^4 - 20\mathsf{X}^3 + 10\mathsf{X} + 20 \in \mathbb{Z}[\mathsf{X}]$. Το $\varphi(\mathsf{X})$ είναι πρωταρχικό υπεράνω τού $\mathbb{Z}$. Μέσω τού κριτηρίου τού Eisenstein διαπιστώνουμε ότι αυτό είναι ανάγωγο τόσον υπεράνω τού $\mathbb{Q}$ όσον και υπεράνω τού $\mathbb{Z}$, καθότι $5 \nmid 3$, $25 \nmid 20$ και το 5 διαιρεί τους ακεραίους $15, -20, 10$ και 20.

5.8 ΑΔΡΟΜΕΡΗΣ ΙΕΡΑΡΧΗΣΗ ΑΚΕΡΑΙΩΝ ΠΕΡΙΟΧΩΝ

Οι ιδιότητες τής διαιρετότητας, οι μελετηθείσες στο παρόν κεφάλαιο, μας οδηγούν στη σύνταξη τού πίνακα τής σελίδας 267, μέσω τού οποίου γίνεται μια (έστω και) αδρομερής ιεράρχηση (διαφόρων ειδών) ακεραίων περιοχών.

5.8.1 Σημείωση. Οι εγκλειστικές σχέσεις (μεταξύ των ποικίλων κλάσεων δακτυλίων) που περιλαμβάνονται σε αυτόν τον πίνακα (από κάτω προς τα επάνω και εξ αριστερών προς τα δεξιά) προκύπτουν από τα εδάφια 2.7.3 (i), 2.3.3, 2.3.2, 5.4.3 (i), 4.2.3, 5.4.21, 5.6.8, 5.6.11, 5.6.13, 5.3.6, 5.6.5 και 5.6.6. (Εξαιρούνται μόνον οι λεγόμενες *περιοχές τού Dedekind*, οι οποίες δεν εστάθη δυνατόν να ορισθούν και να μελετηθούν κατά τη διάρκεια των παραδόσεων λόγω ελλείψεως χρόνου.)

5.8.2 Παραδείγματα. Όλοι οι εγκλεισμοί τού πίνακα είναι *αυστηροί*. Δειγματοληπτικώς (και εκ νέου από κάτω προς τα επάνω και εξ αριστερών προς τα δεξιά) αναφέρουμε τα εξής:

(i) Οι δακτύλιοι $\mathbb{Z}_{\langle p\rangle}$ (όπου p πρώτος) και $K[\![\mathsf{X}]\!]$ (όπου K σώμα) αποτελούν παραδείγματα τοπικών δακτυλίων που δεν είναι σώματα (βλ. 2.7.3 (ii) και (iv)).

(ii) Ο δακτύλιος $\mathbb{H}_{\mathbb{R}}$ των τετρανίων υπεράνω τού σώματος $\mathbb{R}$ είναι ένα στρεβλό σώμα (= διαιρετικός δακτύλιος) που δεν είναι σώμα (βλ. 1.2.19 (ii)).

(iii) Ο δακτύλιος $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ είναι ένας απλός δακτύλιος με μοναδιαίο στοιχείο που δεν είναι στρεβλό σώμα (βλ. προτάσεις 2.3.4 και 1.2.13).

(iv) Ο $\mathbb{Z}$ μπορεί να εφοδιασθεί με ευκλείδειες στάθμες αλλά (προφανώς) δεν είναι σώμα (βλ. 5.4.3 (ii)).

(v) Ο $\mathbb{Z}/m\mathbb{Z}$, όπου m ένας σύνθετος φυσικός αριθμός, είναι ένας μεταθετικός δακτύλιος κυρίων ιδεωδών με μοναδιαίο στοιχείο που δεν είναι ούτε διαιρετικός δακτύλιος ούτε Π.Κ.Ι. (βλ. πόρισμα 4.2.7).

(vi) Ο δακτύλιος $\mathfrak{O}_m$ των ακεραίων τού $\mathbb{Q}(\sqrt{m})$ είναι Π.Κ.Ι. αλλά όχι και ευκλείδεια περιοχή όταν $m \in \{-163, -67, -43, -19\}$ (βλ. πόρισμα 5.5.16).

(vii) Ο δακτύλιος $\mathbb{Z}[\mathsf{X}]$ είναι Π.Μ.Π. αλλά δεν είναι Π.Κ.Ι. (βλ. 5.7.15 (i)).

(viii) Ο δακτύλιος $R := \left\{ z \in \mathbb{C} \,|\, \varphi(z) = 0, \text{ για κάποιο μονικό } \varphi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \smallsetminus \{0_{\mathbb{Z}[\mathsf{X}]}\} \right\}$ είναι μια περιοχή με μ.κ.δ. που δεν είναι Π.Μ.Π.

(ix) Εάν για κάθε $n \in \mathbb{N}_0$ θέσουμε $\xi_n := \sqrt[2^n]{2}$, τότε ορίζεται μια ακεραία περιοχή

$$R_n := \{ \varphi(\xi_n) \,|\, \varphi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \}$$

και σχηματίζεται μια ανιούσα ακολουθία ακεραίων περιοχών

$$\mathbb{Z} = R_0 \subsetneqq R_1 \subsetneqq R_2 \subsetneqq \cdots \subsetneqq R_{n-1} \subsetneqq R_n \subsetneqq \cdots$$

Ο υποδακτύλιος $R := \bigcup_{n\in\mathbb{N}_0} R_n$ τού $\mathbb{R}$ που προκύπτει ως ένωση αυτών είναι ωσαύτως μια ακεραία περιοχή. Αφήνεται ως άσκηση η απόδειξη τού ότι $\xi_n \notin R^{\times}$, $\forall n \in \mathbb{N}_0$, και τού ότι (στην ακολουθία $(\xi_n)_{n\in\mathbb{N}_0}$) ο όρος ξ_{n+1} είναι ένας γνήσιος διαιρέτης τού ξ_n (καθόσον $\xi_{n+1}^2 = \xi_n$). Μέσω αυτής συμπεραίνουμε ότι η ακεραία περιοχή R *δεν πληροί* τη συνθήκη των αλυσίδων γνησίων διαιρετών (βλ. 5.6.4).

(x) Η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-5}]$ είναι περιοχή με παραγοντοποίηση αλλά δεν είναι ούτε περιοχή με μ.κ.δ. ούτε Π.Μ.Π. (βλ. 5.2.42 (iii) και 5.6.7 (i)).

(xi) Έστω $\mathcal{O}(\mathbb{C}) := \{$συναρτήσεις $f : \mathbb{C} \longrightarrow \mathbb{C} \,|\, f$ ολόμορφη$\}$ η ακεραία περιοχή των λεγομένων *ακεραίων συναρτήσεων* μιας μιγαδικής μεταβλητής (βλ. 3.5.6 (iii)). Τα αντιστρέψιμα στοιχεία της είναι οι ακέραιες συναρτήσεις που δεν μηδενίζονται πουθενά. Είναι εύκολο να αποδειχθεί ότι *κάθε ανάγωγο στοιχείο της είναι πρώτο* και ότι το σύνολο των αναγώγων (= πρώτων) στοιχείων της αποτελείται από τις γραμμικές συναρτήσεις τής μορφής $z - a$, $a \in \mathbb{C}$. Ως εκ τούτου, η $\mathcal{O}(\mathbb{C})$ *δεν είναι περιοχή με παραγοντοποίηση*. (Εάν υποθέταμε το αντίθετο, τότε θα έπρεπε *κάθε* $f \in \mathcal{O}(\mathbb{C})$ να γράφεται ως γινόμενο $f = gh_1 \cdots h_k$ μιας πουθενά μηδενιζόμενης συνάρτησης $g \in \mathcal{O}(\mathbb{C})^{\times}$ και πεπερασμένου πλήθους συναρτήσεων τής μορφής

$$h_1(z) = z - a_1, \ldots, h_k(z) = z - a_k,\ k \in \mathbb{N},\ a_1, \ldots, a_k \in \mathbb{C},$$

κάτι που θα ήταν αδύνατο, καθόσον υπάρχουν συναρτήσεις $f \in \mathcal{O}(\mathbb{C})$, όπως, π.χ., η $f(z) = \sin z$, που διαθέτουν άπειρα (σαφώς διακεκριμένα) σημεία τού μιγαδικού επιπέδου ως σημεία μηδενισμού της. Σημειωτέον ότι στο εδάφιο 4.1.14 χρησιμοποιήσαμε παρόμοια επιχειρήματα για να αποδείξουμε ότι η $\mathcal{O}(\mathbb{C})$ *δεν είναι ναιτεριανή*.)

(xii) Για κάθε σώμα K υφίσταται μια ανιούσα ακολουθία ακεραίων περιοχών

$$K[\mathsf{X}_1] \subsetneqq K[\mathsf{X}_1, \mathsf{X}_2] \subsetneqq \cdots \subsetneqq K[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}] \subsetneqq K[\mathsf{X}_1, \ldots, \mathsf{X}_n] \subsetneqq \cdots$$

Ο πολυωνυμικός δακτύλιος άπειρων (αριθμήσιμων, ανεξάρτητων) απροσδιορίστων

$$K[\mathsf{X}_1, \mathsf{X}_2, \ldots, \mathsf{X}_{m-1}, \mathsf{X}_m, \ldots] := \bigcup_{n\in\mathbb{N}} K[\mathsf{X}_1, \ldots, \mathsf{X}_n],$$

που προκύπτει ως ένωση αυτών, είναι μια περιοχή με παραγοντοποίηση (και μάλιστα μια Π.Μ.Π.) αλλά δεν είναι ναιτεριανή περιοχή, διότι το $\langle\{\, \mathsf{X}_n \,|\, n \in \mathbb{N}\}\rangle$ δεν είναι πεπερασμένως παραγόμενο ιδεώδες αυτής (βλ. θεώρημα 4.1.11).

(xiii) Ο $\mathbb{Z}_6$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο που δεν είναι ακεραία περιοχή (βλ. πόρισμα 1.2.27).

(xiv) Ο $2\mathbb{Z}$ είναι ένας μεταθετικός δακτύλιος χωρίς μοναδιαίο στοιχείο (βλ. εδάφιο 1.1.4 (iii)).

$$
\begin{array}{ccccc}
\{\text{Ακέραιες περιοχές}\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} \\
\cup & & & & \cup \\
\left\{\begin{matrix}\text{Περιοχές με}\\ \text{παραγοντοποίηση}\end{matrix}\right\} & \supset & \{\text{Ναιτεριανές περιοχές}\} & \supset & \left\{\begin{matrix}\text{Περιοχές}\\ \text{τού}\\ \text{Dedekind}\end{matrix}\right\} \\
\cup & & & & \\
\left\{\begin{matrix}\text{Περιοχές}\\ \text{που πληρούν}\\ \text{τη συνθήκη}\\ \text{των αλυσίδων}\\ \text{γνησίων}\\ \text{διαιρετών}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Περιοχές,}\\ \text{στις οποίες}\\ \text{κάθε ανάγωγο}\\ \text{στοιχείο}\\ \text{είναι πρώτο}\end{matrix}\right\} & & \\
\cup & & \cup & & \\
\left\{\begin{matrix}\text{Περιοχές}\\ \text{μονοσήμαντης}\\ \text{παραγοντοποιήσεως}\\ \text{(Π.Μ.Π)}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Περιοχές με}\\ \text{μ.κ.δ.}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\\ \text{(Δ.Κ.Ι)}\end{matrix}\right\} \\
\cup & & & & \cup \\
\left\{\begin{matrix}\text{Περιοχές κυρίων}\\ \text{ιδεωδών (Π.Κ.Ι)}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\end{matrix}\right\} & & \left\{\begin{matrix}\text{1-δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\end{matrix}\right\} \\
\cup & & & & \\
\{\text{Ευκλείδειες περιοχές}\} & & & & \cup \\
\cup & & & & \\
\{\text{Σώματα}\} & \subset & \left\{\begin{matrix}\text{Στρεβλά}\\ \text{σώματα}\end{matrix}\right\} & = & \left\{\begin{matrix}\text{Διαιρετικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} \\
\parallel & & \cap & & \\
\left\{\begin{matrix}\text{Απλοί μεταθετικοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Απλοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & & \\
\cap & & & & \\
\left\{\begin{matrix}\text{Τοπικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} & & & &
\end{array}
$$