ΚΕΦΑΛΑΙΟ 3

Ομομορφισμοί δακτυλίων

Οι απεικονίσεις μεταξύ δυο δακτυλίων, οι οποίες τυγχάνει να είναι συμβατές προς τις εκάστοτε θεωρούμενες πράξεις προσθέσεως και πολλαπλασιασμού, 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 η

$$f : R \longrightarrow R'$$

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

$$\boxed{f(a+b) = f(a) + f(b)} \qquad \text{και} \qquad \boxed{f(ab) = f(a)\, f(b)} \tag{3.1}$$

για όλα τα $a, b \in R$.

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

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιριπτική,
ενδομορφισμός (τού R)	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$R = R'$,
αυτομορφισμό (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 $\text{χαρ}(K) = p > 0$, τότε η απεικόνιση

$$f : K \longrightarrow K, \quad x \longmapsto f(x) := x^p,$$

είναι ένας ενδομορφισμός (πρβλ. πρόταση 1.4.8 (i)) και καλείται, ιδιαιτέρως, **απεικόνιση τού Frobenius**.

(v) Ο ομομορφισμός

$$\mathbb{C} \longrightarrow \mathbb{C}, \;\; z = a + ib \longmapsto a - ib = \overline{z},$$

είναι ένας αυτομορφισμός τού σώματος των μιγαδικών αριθμών.

(vi) Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων και

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

το αριθμητικό τετραγωνικό σώμα το αντιστοιχιζόμενο στον m (βλ. άσκηση **1-37**). 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 δακτυλίων R και S, όπου $f(a) = 0$ για κάθε $a \in R$, είναι ένας ομομορφισμός δακτυλίων (*μηδενικός ομομορφισμός*). Σημειωτέον ότι όταν κανείς εκ των R, S δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιρριπτικός.

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. *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). □

3.1.5 Ορισμός. Εάν οι R και R' είναι δυο δακτύλιοι, τότε γράφουμε[1] $R \cong R'$ και λέμε ότι **ο** R **είναι ισόμορφος με τον** R' (ή ότι οι R και R' **είναι ισόμορφοι**) όταν υπάρχει ισομορφισμός δακτυλίων $f : R \longrightarrow R'$. (Κατ' αναλογίαν, το σύμβολο $R \ncong R'$ δηλοί ότι ο δακτύλιος R *δεν είναι ισόμορφος* με τον R'.)

3.1.6 Παραδείγματα. (i) Η ακεραία περιοχή $\mathbb{Z}[\sqrt{2}]$ (βλ. άσκηση **1-37**) είναι ισόμορφη με τον ακόλουθο δακτύλιο 2×2-πινάκων:

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

καθόσον υφίσταται ισομορφισμός δακτυλίων:

$$\mathbb{Z}[\sqrt{2}] \ni a + b\sqrt{2} \longmapsto \left(\begin{array}{cc} a & b \\ 2b & a \end{array} \right) \in R.$$

(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 $f(i) \in \mathbb{R}$.

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

(i) $R \cong R$,

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

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

[1] Από τούδε και στο εξής μέσω τού συμβόλου "$\cong$" θα εκφράζουμε την ύπαρξη ισομορφισμών *δακτυλίων*. Ωστόσο, επειδή (στη Θεωρία Ομάδων) χρησιμοποιήσαμε το *ίδιο* σύμβολο *και* για τους ισομορφισμούς *ομάδων*, οφείλουμε να είμαστε ιδιάτερα προσεκτικοί (πρβλ. 3.1.2 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.

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

3.1.8 Σημείωση. Σύμφωνα με την πρόταση 3.1.7, η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από δακτυλίους (ή επί τής NBG-«κλάσεως» *όλων* των δακτυλίων). Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο δακτύλιοι λογίζονται ως (δακτυλιοθεωρητικώς) *ταυτιζόμενοι* όταν είναι μεταξύ τους ισόμορφοι, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο δακτυλιοθεωρητικός προσδιορισμός μιας οικογενείας δακτυλίων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού* [2].

3.1.9 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*:

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

(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 $f(1_R) = 1_{f(R)}$.*

[2] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (δακτυλίων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

(vi) *Εάν ο R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, η f μη μηδενικός ομομορφισμός και ο R' διαιρετικός δακτύλιος ή ακεραία περιοχή, τότε $f(1_R) = 1_{R'}$.*

(vii) *Εάν ο R είναι ένας μεταθετικός δακτύλιος, τότε και ο $f(R)$ είναι μεταθετικός.*

(viii) *Εάν ο R είναι ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο και η f μη μηδενικός ομομορφισμός, τότε*

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

και, γενικότερα,

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

(ix) *Εάν η f είναι μονομορφισμός και ο R ακεραία περιοχή (και αντιστοίχως, στεβλό σώμα/σώμα), τότε και ο $f(R)$ είναι ακεραία περιοχή (και αντιστοίχως, στρεβλό σώμα/σώμα).*

ΑΠΟΔΕΙΞΗ. (i) Προφανώς, $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, οπότε ισχύει η ισότητα $f(0_R) = 0_{R'}$. Εξάλλου, για κάθε $a \in R$, έχουμε

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

(ii) Η απόδειξη έπεται από την πρόταση 3.1.3 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

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

οπότε ο $f(R)$ είναι δακτύλιος με μοναδιαίο στοιχείο και $f\left(1_R\right) = 1_{f(R)}$.

(vi) Επειδή -εξ υποθέσεως- ο f δεν είναι ο μηδενικός ομομορφισμός, θα υπάρχει ένα $a \in R$, τέτοιο ώστε $f(a) \neq 0_{R'}$. Εξ αυτού έπεται ότι

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

Εάν ο R είναι διαιρετικός δακτύλιος, τότε υπάρχει το αντίστροφο $f(a)^{-1}$ τού $f(a)$, με το οποίο μπορούμε να πολλαπλασιάσουμε αμφότερα τα μέλη τής ανωτέρω ισότητας και να λάβουμε $f\left(1_R\right) = 1_{R'}$. Εάν, από την άλλη μεριά, ο R είναι ακεραία περιοχή, τότε μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα κάνοντας χρήση τού νόμου τής διαγραφής 1.2.5.

(vii) Προφανώς, για κάθε $a, b \in R$, έχουμε

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

(viii) Για κάθε $a \in R^\times$ έχουμε

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_R) = f(a^{-1}a) = f(a^{-1})f(a).$$

Κι επειδή (λόγω το (v)) ισχύει $f\left(1_R\right) = 1_{f(R)} \neq 0_{R'}$, έχουμε $f(a) \neq 0_{R'}$ και $f(a^{-1}) = \left[f\left(a\right)\right]^{-1} \in f\left(R\right)^\times$. Η δεύτερη ισότητα αποδεικνύεται εύκολα μέσω μαθηματικής επαγωγής.

(ix) Έστω ότι ο f είναι μονομορφισμός και ο R ακεραία περιοχή. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Εάν υποθέσουμε ότι $f(a), f(b) \in f(R)$, για κάποια $a, b \in R$, ούτως ώστε να ισχύει

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

τότε $ab = 0_R$, οπότε $a = 0_R$ ή $b = 0_R$. Συνεπώς, $f(a) = 0_{f(R)}$ ή $f(b) = 0_{f(R)}$. Άρα *και* ο $f(R)$ είναι ακεραία περιοχή.

Εν συνεχεία, ας υποθέσουμε ότι ο f είναι μονομορφισμός και ο R στρεβλό σώμα. Προφανώς, επειδή $1_R \neq 0_R$, το $f(1_R) = 1_{f(R)}$ είναι διάφορο τού $f(0_R) = 0_{R'}$. Αρκεί λοιπόν να δείξουμε ότι $f(R)^\times = f(R) \setminus \{0_{R'}\}$. Ο εγκλεισμός "$\subseteq$" είναι πρόδηλος. Ας θεωρήσουμε τυχόν $b \in f(R) \setminus \{0_{R'}\}$. Τότε υπάρχει ένα $a \in R \setminus \{0_R\}$, τέτοιο ώστε $b = f(a)$. Όμως -εξ υποθέσεως- $R \setminus \{0_R\} = R^\times$, οπότε $a \in R^\times$, πράγμα που σημαίνει ότι υπάρχει (πολλαπλασιαστικό) αντίστροφο a^{-1} τού a, για το οποίο ισχύει $f(a^{-1}) = \left[f\left(a\right)\right]^{-1} \in f\left(R\right)^\times$ (βάσει τού (viii)). Άρα $b \in f(R)^\times$, και, ως εκ τούτου, ο $f(R)$ είναι στρεβλό σώμα. (Στην περίπτωση κατά την οποία ο f είναι μονομορφισμός και ο R σώμα, αρκεί να χρησιμοποιήσουμε ό,τι προείπαμε σε συνδυασμό με το (vii).) □

3.1.10 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 εφαρμοσθε το (ix) τής προτάσεως 3.1.9 για αμφότερες τις f και f^{-1}. (Πρβλ. με το (ii) τής προτάσεως 3.1.7.) □

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 3.1.9, 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. □

3.1.13 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 $a, b \in \text{Ker}(f)$. Τότε

$$\left.\begin{array}{r} f(a-b) = f(a) - f(b) = 0_{R'} - 0_{R'} = 0_{R'}, \\ f(ar) = f(a)f(r) = 0_{R'} f(r) = 0_{R'}, \\ f(ra) = f(r)f(a) = f(r)0_{R'} = 0_{R'} \end{array}\right\} \Longrightarrow a-b,\ ar,\ ra \in \text{Ker}(f).$$

Άρα ο $\text{Ker}(f)$ είναι εξ ορισμού ένα ιδεώδες τού R. □

3.1.15 Πρόταση. *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Τότε ο*

$$f \text{ είναι μονομορφισμός} \iff \text{Ker}\,(f) = \{0_R\}\ .$$

ΑΠΟΔΕΙΞΗ. Εάν ο f είναι μονομορφισμός δακτυλίων και a είναι ένα τυχόν στοιχείο τού πυρήνα $\text{Ker}(f)$, τότε

$$f(a) = 0_{R'} = f(0_R) \underset{f \text{ ένριψη}}{\Longrightarrow} a = 0_R.$$

Άρα $\text{Ker}(f) = \{0_R\}$. Και αντιστρόφως· εάν ισχύει $\text{Ker}(f) = \{0_R\}$ και υποθέσουμε ότι $f(x) = f(y)$, για κάποια $x, y \in R$, τότε

$$f(x-y) = f(x) - f(y) = 0_{R'} \Longrightarrow x - y \in \text{Ker}(f) = \{0_R\} \Longrightarrow x - y = 0_R,$$

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 $f : R \longrightarrow R'$. Θέτοντας $S := f(R)$, γνωρίζουμε ότι ο S είναι υποδακτύλιος τού R' (βλ. 3.1.9 (iii)). Περιορίζοντας το πεδίο τιμών τού f στην εικόνα του λαμβάνουμε τον ισομορφισμό

$$R \ni r \longmapsto f(r) \in S.$$

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* $\text{χαρ}(R') = 0$ *ή* $\text{χαρ}(R') = \text{χαρ}(R)$.

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

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

είναι ένας μονομορφισμός. Εάν $\text{χαρ}(R) = k > 0$, τότε μπορούμε να θεωρήσουμε ως R' το καρτεσιανό γινόμενο $R' := \mathbb{Z}_k \times R$ εφοδιασμένο με τις πράξεις:

(i) $([m]_k, a) + ([n]_k, b) := ([m + n]_k, a + b)$,

(ii) $([m]_k, a) \cdot ([n]_k, b) := ([mn]_k, mb + na + ab)$,

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

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

είναι και πάλι ένας μονομορφισμός. □

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 $n \in \mathbb{Z} \setminus \{0\}$ 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

$$\boxed{\varpi : R \longrightarrow R/I, \;\; \varpi\,(r) := r + I, \; \forall r \in R,} \tag{3.4}$$

είναι προφανώς επιριπτική.

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 $\mathrm{Ker}(\varpi) = \{\, r \in R \mid r + I = I \} = I$. 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 $\varpi : R \longrightarrow R/I$ 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 $\varpi : R \longrightarrow R/I$, ο οποίος είναι μη μηδενικός με $\mathrm{Ker}(\varpi) = I$. Εάν υποθέσουμε ότι ο ϖ 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 $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, 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 Θεώρημα τής αντιστοιχίσεως. *Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων και έστω $W := \mathrm{Ker}(f)$. Τότε η*

$$\left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } R\\ \text{τα οποία περιέχουν τον } W\end{array}\right\} \xrightarrow{F} \left\{\begin{array}{c}\text{αριστερά/δεξιά/αμφίπλευρα}\\ \text{ιδεώδη τού } S\end{array}\right\}$$

$$I \longmapsto f(I)$$

είναι αμφιρριπτική απεικόνιση και διατηρεί την εγκλειστική σχέση, ήτοι

$$(W \subseteq)\ I_1 \subsetneqq I_2 \Longleftrightarrow f(I_1) \subsetneqq f(I_2).$$

ΑΠΟΔΕΙΞΗ. Το ότι η F είναι καλώς ορισμένη απεικόνιση έπεται από το (i) τού λήμματος 3.2.1. Για να αποδείξουμε ότι η F είναι *επιρριπτική* αρκεί να αποδείξουμε ότι κάθε (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες J τού S είναι τής μορφής $f(I)$, όπου I ένα (αριστερό/δεξιό/αμφίπλευρο) ιδεώδες τού R. Τούτο έπεται από το ότι $J = f(f^{-1}(J))$, όπου το $I = f^{-1}(J)$ είναι ομοειδές ιδεώδες (βλ. 3.2.1 (ii)). Σημειωτέον ότι ο εγκλεισμός $J \supseteq f(f^{-1}(J))$ είναι προφανής (από τη Θεωρία Συνόλων). Έστω $b \in J$. Επειδή η f είναι επιρριπτική, υπάρχει $a \in R$, τέτοιο ώστε $b = f(a)$. Κατά συνέπειαν,

$$a \in f^{-1}(J) \Longrightarrow b = f(a) \in f(f^{-1}(J)),$$

οπότε και $J \subseteq f(f^{-1}(J))$. Εν συνεχεία, θα αποδείξουμε ότι η F είναι και *ενριπτική*. Ας υποθέσουμε ότι τα I_1, I_2 είναι δυο (αριστερά/δεξιά/αμφίπλευρα) ιδεώδη τού R τα οποία περιέχουν τον πυρήνα W και για τα οποία ισχύει η ισότητα

$$F(I_1) = F(I_2) \Longrightarrow f(I_1) = f(I_2).$$

Θα αποδείξουμε την ισότητα $I_1 = f^{-1}(f(I_1))$. Ο εγκλεισμός $I_1 \subseteq f^{-1}(f(I_1))$ είναι προφανής (από τη Θεωρία Συνόλων). Έστω $a \in f^{-1}(f(I_1))$. Τότε $f(a) \in f(I_1)$, οπότε υπάρχει ένα $x \in I_1$, τέτοιο ώστε $f(a) = f(x)$. Κατά συνέπειαν,

$$\left.\begin{array}{r} x - a \in W \subseteq I_1 \\ x \in I_1 \end{array}\right\} \Longrightarrow x - (x - a) = a \in I_1,$$

δηλαδή $I_1 \supseteq f^{-1}(f(I_1))$. Άρα πράγματι $I_1 = f^{-1}(f(I_1))$. Αναλόγως αποδεικνύουμε ότι $I_2 = f^{-1}(f(I_2))$. Εξ αυτών έπεται ότι

$$f(I_1) = f(I_2) \Longrightarrow I_1 = f^{-1}(f(I_1)) = f^{-1}(f(I_2)) = I_2,$$

ήτοι η ενριπτικότητα τής F. Τέλος, ας υποθέσουμε ότι τα I_1, I_2 είναι δυο (αριστερά/δεξιά/αμφίπλευρα) ιδεώδη τού R τα οποία περιέχουν τον πυρήνα W και για τα οποία ισχύει ο εγκλεισμός $I_1 \subsetneqq I_2$. Τότε $f(I_1) \subseteq f(I_2)$. Εάν ίσχυε η ισότητα $f(I_1) = f(I_2)$, θα καταλήγαμε (όπως επιχειρηματολογήσαμε προηγουμένως) στην (εξ υποθέσεως) άτοπη ισότητα $I_1 = I_2$. Άρα $f(I_1) \subsetneqq f(I_2)$. Και αντιστρόφως· εάν $f(I_1) \subsetneqq f(I_2)$, τότε

$$I_1 = f^{-1}(f(I_1)) \subsetneqq f^{-1}(f(I_2)) = I_2 \Longrightarrow I_1 \subsetneqq I_2,$$

απ' όπου έπεται ότι και η αντίστροφη συνεπαγωγή είναι αληθής. □

3.2.4 Πόρισμα. *Έστω I ένα ιδεώδες ενός δακτυλίου R. Τότε κάθε ιδεώδες τού πηλικοδακτυλίου R/I είναι τής μορφής J/I, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το I.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τον φυσικό επιμορφισμό $\varpi : R \longrightarrow R/I$ (βλ. (3.4)). Βάσει τού θεωρήματος 3.2.3 τής αντιστοιχίσεως ιδεωδών κάθε ιδεώδες τού R/I είναι τής μορφής $\varpi(J)$, όπου J κάποιο (μονοσημάντως ορισμένο) ιδεώδες τού R το οποίο περιέχει το $I = \mathrm{Ker}(\varpi)$ (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 $\varpi(J)$ ισούται με

$$\varpi(J) = \{\, \varpi(a) \mid a \in J \} = \{\, a + I \mid a \in J \} = J/I,$$

απ' όπου έπεται το ζητούμενο. □

3.2.5 Παράδειγμα. Για $R = \mathbb{Z}$ και $I = m\mathbb{Z}$, $m \in \mathbb{N}$, το σύνολο των ιδεωδών τού πηλικοδακτυλίου $\mathbb{Z}/m\mathbb{Z}$ είναι το

$$\{\, d\mathbb{Z}/m\mathbb{Z} \mid \ d \in \mathbb{N} \text{ και } d \mid m \,\}.$$

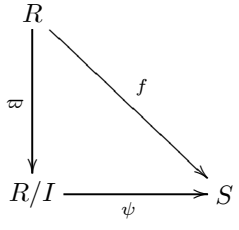
3.3 ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Αυτά είναι τρία χαρακτηριστικά θεωρήματα (βλ. 3.3.2, 3.3.14 και 3.3.19) 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 Θεώρημα. *Έστω ότι ο* $f : R \longrightarrow S$ *είναι ένας ομομορφισμός δακτυλίων, το* I *ένα ιδεώδες τού* R*, τέτοιο ώστε* $I \subseteq \mathrm{Ker}(f)$*, και* $\varpi : R \longrightarrow R/I$ *ο φυσικός επιμορφισμός* (3.4)*. Τότε η*

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

είναι καλώς ορισμένη απεικόνιση και αποτελεί έναν ομομορφισμό δακτυλίων ο οποίος καθιστά το διάγραμμα



μεταθετικό (ήτοι $\psi \circ \varpi = f$*). Η απεικόνιση* ψ *είναι επιρριπτική εάν και μόνον εάν η* f *είναι επιρριπτική, ενώ είναι ενριπτική εάν και μόνον εάν ισχύει η ισότητα* $I = \mathrm{Ker}(f)$.

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

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

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

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

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

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

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

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

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

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

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

($\Longleftarrow$) Εάν υποθέσουμε ότι $\text{Ker}(f) = I$, αρκεί να δείξουμε (επί τη βάσει τής προτάσεως 3.1.15) ότι $\text{Ker}(\psi) = \{0_{R/I}\}$. Έστω λοιπόν τυχόν $a + I \in \text{Ker}(\psi)$. Τότε

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

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

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

$$\psi : R/\text{Ker}(f) \longrightarrow \text{Im}\,(f) = f\,(R)\,, \quad a + \text{Ker}(f) \longmapsto f\,(a)\,,\ \forall a \in R,$$

είναι ισομορφισμός δακτυλίων, ήτοι

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

ΑΠΟΔΕΙΞΗ. Άμεση δυνάμει τού θεωρήματος 3.3.1, όταν θέσουμε $I := \text{Ker}(f)$. □

3.3.3 Παραδείγματα. (i) Έστω $m \in \mathbb{N}$ και έστω f ο επιμορφισμός δακτυλίων

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_m,\ \ n \longmapsto [n]_m\,,\ \ \forall n \in \mathbb{Z}.$$

Τότε

$$\begin{aligned} \text{Ker}\,(f) &= \{r \in \mathbb{Z} \mid\ f(r) = [0]_m\} = \{r \in \mathbb{Z} \mid [r]_m = [0]_m\} \\ &= \{r \in \mathbb{Z} \mid r = km,\ k \in \mathbb{Z}\} = \{km \mid k \in \mathbb{Z}\} = m\mathbb{Z}, \end{aligned}$$

και, σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.2, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Εξάλλου, επειδή $m\mathbb{Z} = -m\mathbb{Z}$ για κάθε $m \in \mathbb{Z}\setminus\{0\}$, έχουμε γενικότερα

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_{|m|},\ \forall m \in \mathbb{Z}\setminus\{0\}.} \tag{3.5}$$

(ii) Έστω R ο υποδακτύλιος τού $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ ο οριζόμενος ως εξής:

$$R := \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \;\middle|\; a, b \in \mathbb{R} \right\},$$

και έστω f η επιρριπτική απεικόνιση

$$f : R \longrightarrow \mathbb{R},\ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \longmapsto a.$$

Τότε -όπως κανείς μπορεί εύκολα να ελέγξει- η f είναι ομομορφισμός δακτυλίων, οπότε, δυνάμει τού 1ου θεωρήματος ισομορφισμών 3.3.2,

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

όπου

$$I = \mathrm{Ker}\,(f) = \left\{ \left(\begin{array}{cc} 0 & b \\ 0 & 0 \end{array} \right) \;\middle|\; b \in \mathbb{R} \right\}.$$

(iii) Έστω R ο υποδακτύλιος τού σώματος $\mathbb{Q}$ των ρητών αριθμών ο οριζόμενος ως εξής:

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

Η επιρριπτική απεικόνιση

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

είναι ομομορφισμός δακτυλίων (γιατί;) και (βάσει τού 1ου θεωρήματος ισομορφισμών 3.3.2)

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

(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 $\mathbb{Z}[\mathsf{X}]$.

3.3.4 Πόρισμα. *Έστω ότι ο $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και το I ένα ιδεώδες τού R, τέτοιο ώστε $I \subseteq \mathrm{Ker}(f)$. 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 $\varpi : S \longrightarrow S/f(I)$ ο φυσικός επιμορφισμός τού S επί τού πηλικοδακτυλίου $S/f(I)$. Η απεικόνιση $g = \varpi \circ f : R \longrightarrow S/f(I)$ είναι ένας επιμορφισμός δακτυλίων (ως σύνθεση δύο επιμορφισμών, βλ. 3.1.4) με πυρήνα του το ιδεώδες

$$\begin{aligned}
\mathrm{Ker}\,(g) &= \left\{ a \in R \mid\ g(a) = 0_{S/f(I)} \right\} \\
&= \{ a \in R \mid\ \varpi(f(a)) = f(I) \} \\
&= \{ a \in R \mid\ f(a) + f(I) = f(I) \} \\
&= \{ a \in R \mid\ f(a) \in f(I) \} \\
&= f^{-1}(f(I)),
\end{aligned}$$

το οποίο ισούται με το I (βλ. απόδειξη τού θεωρήματος 3.2.3). Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.2 για την g. □

3.3.5 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 $\varpi : S \longrightarrow S/J$ ο φυσικός επιμορφισμός τού S επί τού πηλικοδακτυλίου S/J. Η απεικόνιση $g = \varpi \circ f : R \longrightarrow S/J$ είναι ένας επιμορφισμός δακτυλίων (ως σύνθεση δύο επιμορφισμών, βλ. 3.1.4), με πυρήνα του το ιδεώδες

$$\begin{aligned}
\mathrm{Ker}\,(g) &= \left\{ a \in R \mid\ g(a) = 0_{S/J} \right\} \\
&= \{ a \in R \mid\ \varpi(f(a)) = J \} \\
&= \{ a \in R \mid\ f(a) + J = J \} \\
&= \{ a \in R \mid\ f(a) \in J \} \\
&= f^{-1}(J).
\end{aligned}$$

Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.2 για την g. □

3.3.6 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 3.3.4). 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 3.3.5 και τού (ii) τής προτάσεως 3.1.7). 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 $\mathrm{Ker}(f) \subseteq f^{-1}(\mathfrak{q})$. □

3.3.7 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*

$$\mathrm{Spec}(R) := \{\,\mathfrak{p} \mid \mathfrak{p} \text{ πρώτο ιδεώδες τού } R\}\,,\ \mathrm{Spec}(S) := \{\,\mathfrak{q} \mid \mathfrak{q} \text{ πρώτο ιδεώδες τού } S\}$$

των R *και* S (βλ. άσκηση **2-36**). *Εάν* $\mathrm{Spec}(S) \neq \varnothing$, *τότε η*

$$\begin{array}{ccc} \mathbf{V}(W) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq W\} & \longrightarrow & \mathrm{Spec}(S) \\ \mathfrak{p} & \longmapsto & f(\mathfrak{p}) \end{array} \tag{3.6}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$(W \subseteq)\ \mathfrak{p}_1 \subsetneqq \mathfrak{p}_2 \Longleftrightarrow f(\mathfrak{p}_1) \subsetneqq f(\mathfrak{p}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.6, 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 3.2.3), η (3.6) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός $F|_{\mathbf{V}(W)}$ τής F τής ορισθείσας στο θεώρημα 3.2.3 επί τού $\mathbf{V}(W)$). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.3. □

3.3.8 Σημείωση. Εάν ο $f : R \longrightarrow S$ ένας ομομορφισμός (όχι κατ' ανάγκην επιμορφισμός!) μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, τότε

$$f^{-1}(\mathfrak{q}) \in \text{Spec}(R), \ \ \forall \mathfrak{q} \in \text{Spec}(S),$$

οπότε, υπό την προϋπόθεση ότι $\text{Spec}(S) \neq \varnothing$, ο f επάγει μια «κανονιστική» απεικόνιση (σε επίπεδο πρώτων φασμάτων):

$$\text{Spec}(S) \ni \mathfrak{q} \longmapsto f^{-1}(\mathfrak{q}) \in \text{Spec}(R).$$

Πράγματι· η αντίστροφη εικόνα $f^{-1}(\mathfrak{q})$ οιουδήποτε $\mathfrak{q} \in \text{Spec}(S)$ είναι ένα ιδεώδες τού R (βλ. 3.2.1 (ii)), ο πηλικοδακτύλιος $S/\mathfrak{q}$ είναι ακεραία περιοχή (βλ. θεώρημα 2.6.4) και η εφαρμογή τού 1ου θεωρήματος ισομορφισμών 3.3.2 για τη σύνθεση $\varpi \circ f$ των ομομορφισμών

$$R \xrightarrow{f} S \xrightarrow{\varpi} S/\mathfrak{q}$$

(όπου $\varpi : S \longrightarrow S/\mathfrak{q}$ ο φυσικός επιμορφισμός) δίδει τον ισομορφισμό

$$R/\text{Ker}(\varpi \circ f) \cong \text{Im}(\varpi \circ f) \subseteq S/\mathfrak{q}.$$

Επειδή (σύμφωνα με το (iii) τής προτάσεως 3.1.9) η εικόνα $\text{Im}(\varpi \circ f)$ είναι ένας υποδακτύλιος τής ακεραίας περιοχής $S/\mathfrak{q}$ και

$$1_{S/\mathfrak{q}} = 1_S + \mathfrak{q} = \varpi(1_S) = \varpi(f(1_R)) = (\varpi \circ f)(1_R) = 1_{\text{Im}(\varpi \circ f)}$$

(βλ. 3.1.9 (v)), η πρόταση 1.2.20 μας πληροφορεί ότι η $\text{Im}(\varpi \circ f)$ είναι ακεραία περιοχή, οπότε και ο πηλικοδακτύλιος $R/\text{Ker}(\varpi \circ f)$ είναι ακεραία περιοχή (σύμφωνα με το (i) τού πορίσματος 3.1.10). Επιπροσθέτως, επειδή

$$\begin{aligned} \text{Ker}(\varpi \circ f) &= \left\{ r \in R \mid \varpi\left(f\left(r\right)\right) = 0_{S/\mathfrak{q}} \right\} \\ &= \left\{ r \in R \mid f\left(r\right) + \mathfrak{q} = \mathfrak{q} \right\} \\ &= \left\{ r \in R \mid f\left(r\right) \in \mathfrak{q} \right\} = f^{-1}(\mathfrak{q}), \end{aligned}$$

ο πηλικοδακτύλιος $R/f^{-1}(\mathfrak{q})$ είναι μια ακεραία περιοχή, οπότε έχουμε κατ' ανάγκην $f^{-1}(\mathfrak{q}) \in \text{Spec}(R)$ (βλ. θεώρημα 2.6.4).

3.3.9 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 3.3.7 και 3.2.4. □

3.3.10 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 3.3.4). 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 3.3.4, και τού (ii) τής προτάσεως 3.1.7). 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 3.3.7 *για μεγιστικά ιδεώδη*.

3.3.11 Πόρισμα. (Θεώρημα αντιστοιχίσεως για μεγιστικά ιδεώδη.)
Έστω $f : R \longrightarrow S$ ένας επιμορφισμός μεταθετικών δακτυλίων με μοναδιαία στοιχεία. Θέτουμε $W := \mathrm{Ker}(f)$ και θεωρούμε τα ***μεγιστικά φάσματα***

$$\text{Max-Spec}(R) := \left\{ \mathfrak{m} \;\middle|\; \begin{array}{c} \mathfrak{m} \text{ μεγιστικό} \\ \text{ιδεώδες τού } R \end{array} \right\}, \quad \text{Max-Spec}(S) := \left\{ \mathfrak{n} \;\middle|\; \begin{array}{c} \mathfrak{n} \text{ μεγιστικό} \\ \text{ιδεώδες τού } S \end{array} \right\}$$

των R και S. Εάν ο S είναι μη τετριμμένος, τότε η

$$\boxed{\begin{array}{ccc} \{\mathfrak{m} \in \text{Max-Spec}(R) \,|\mathfrak{m} \supseteq W\} & \longrightarrow & \text{Max-Spec}(S) \\ \mathfrak{m} & \longmapsto & f(\mathfrak{m}) \end{array}} \tag{3.7}$$

είναι αμφιρριπτική απεικόνιση η οποία διατηρεί την εγκλειστική σχέση, ήτοι

$$(W \subseteq)\ \mathfrak{m}_1 \subsetneqq \mathfrak{m}_2 \Longleftrightarrow f(\mathfrak{m}_1) \subsetneqq f(\mathfrak{m}_2).$$

ΑΠΟΔΕΙΞΗ. Κατά το πόρισμα 3.3.10, το $f(\mathfrak{m})$ είναι ένα μεγιστικό ιδεώδες τού 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 3.2.3), η (3.7) είναι αμφιρριπτική απεικόνιση (και μάλιστα, εκ κατασκευής, ο περιορισμός τής F τής ορισθείσας στο θεώρημα 3.2.3 επί τού συνόλου των μεγιστικών ιδεωδών τού R που περιέχουν τον W). Η διατήρηση τής εγκλειστικής σχέσεως αποδεικνύεται όπως στο θεώρημα 3.2.3. □

3.3.12 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. 3.3.8), 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 $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, παρατηρούμε ότι η ι είναι μονομορφισμός, δεν είναι επιμορφισμός, $\iota(1) = 1$, το τετριμμένο ιδεώδες $\{0\}$ τού $\mathbb{Q}$ είναι μεγιστικό (βλ. πόρισμα 2.1.11), αλλά η αντίστροφη εικόνα $\iota^{-1}(\{0\}) = \{0\}$ τού $\{0\}$ είναι το τετριμμένο ιδεώδες τού δακτυλίου $\mathbb{Z}$ των ακεραίων αριθμών που *δεν είναι μεγιστικό ιδεώδες* (βλ. 2.5.23 (i)).

3.3.13 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 3.3.11 και 3.2.4. □

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

(i) *το $S \cap I$ είναι ένα ιδεώδες τού S,*

(ii) *το*

$$S + I := \{\, s + a \mid \ s \in S,\ a \in I\}$$

είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$,

(iii) *το I είναι ένα ιδεώδες τού $S + I$ και*

(iv) *υφίσταται ισομορφισμός δακτυλίων*

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

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

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

Επίσης, το $S \cap I$ αποτελεί προσθετική υποομάδα τής (αβελιανής) ομάδας $(S, +)$. Έστω τώρα τυχόν $a \in S \cap I$. Προφανώς, $a \in S$ και $a \in I$. Επειδή $a \in S$ και ο S είναι υποδακτύλιος τού R, ισχύει

$$sa \in S, \;\; as \in S, \; \forall s \in S,$$

λόγω τής κλειστότητας τής πράξεως τού πολλαπλασιασμού εντός τού S. Από την άλλη μεριά, επειδή το I είναι ιδεώδες τού R,

$$sa \in I, \;\; as \in I.$$

Επομένως, $sa, as \in S \cap I$ για κάθε $s \in S$ και κάθε $a \in S \cap I$. Εξ αυτών έπεται ότι το $S \cap I$ είναι ένα ιδεώδες τού S.

(ii) Εάν $s \in S$, τότε προφανώς $s + 0_R \in S + I$, αφού $0_R \in I$. Άρα $S \subseteq S + I$. Εν συνεχεία, ας υποθέσουμε ότι $x_1, x_2 \in S + I$. Τα x_1, x_2 γράφονται ως $x_1 = s_1 + a_1$ και $x_2 = s_2 + a_2$, για κάποια $s_1, s_2 \in S$ και $a_1, a_2 \in I$. Επομένως,

$$\left.\begin{aligned} x_1x_2 = s_1s_2 + s_1a_2 + a_1s_2 + a_1a_2, \\ s_1s_2 \in S, \\ s_1a_2 + a_1s_2 + a_1a_2 \in I \end{aligned}\right\} \Longrightarrow x_1x_2 \in S + I,$$

και

$$\left.\begin{aligned} x_1 - x_2 = (s_1 - s_2) + (a_1 - a_2)\,, \\ s_1 - s_2 \in S, \\ a_1 - a_2 \in I \end{aligned}\right\} \Longrightarrow x_1 - x_2 \in S + I.$$

Άρα τελικώς το $S + I$ είναι ένας υποδακτύλιος τού R με $S \subseteq S + I$.

(iii) Έστω ότι $a, b \in I$ και $x = s + c \in S + I$, όπου $s \in S$ και $c \in I$. Τότε ο ισχυρισμός είναι αληθής λόγω τής συνεπαγωγής:

$$\left.\begin{aligned} a - b \in I \;\; (\text{διότι το } I \text{ είναι ιδεώδες τού } R) \\ sa \in I \;\; (\text{διότι } s \in R \text{ και το } I \text{ είναι ιδεώδες τού } R) \\ ca \in I \;\; (\text{διότι το } I \text{ είναι υποδακτύλιος τού } R) \end{aligned}\right\} \Longrightarrow a - b, \;\; xa \in I.$$

(iv) Έστω f η απεικόνιση

$$f : S \longrightarrow (S + I)/I, \;\; s \longmapsto s + I, \;\; \forall s \in S.$$

Προφανώς, $f = \varpi \circ j$, όπου $\varpi : S + I \longrightarrow (S + I)/I$ ο επιμορφισμός κλάσεων υπολοίπων και $j : S \longrightarrow S + I$ η συνήθης ένθεση $s \longmapsto s(+0_R)$. Κατά το 1ο

θεώρημα ισομορφισμών 3.3.2, $S/\mathrm{Ker}(f) \cong f(S)$. Θα αποδείξουμε εν πρώτοις ότι $\mathrm{Ker}(f) = S \cap I$. Έστω λοιπόν τυχόν $s \in \mathrm{Ker}(f)$. Τότε

$$f(s) = s + I = 0_R + I \Longrightarrow \left.\begin{array}{r} s \in I \\ s \in S \end{array}\right\} \Longrightarrow s \in S \cap I.$$

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. □

3.3.15 Πόρισμα. *Έστω ότι ο R είναι ένας δακτύλιος και τα I, J δύο ιδεώδη του. Τότε υφίστανται ισομορφισμοί*:

$$\boxed{I/\left(I \cap J\right) \cong \left(I + J\right)/J}$$

και

$$\boxed{\left(I + J\right)/\left(I \cap J\right) \cong \left(\left(I + J\right)/I\right) \times \left(\left(I + J\right)/J\right) \cong \left(J/\left(I \cap J\right)\right) \times \left(I/\left(I \cap J\right)\right)}$$

ΑΠΟΔΕΙΞΗ. Ο πρώτος ισομορφισμός είναι άμεσος δυνάμει τού 2ου θεωρήματος ισομορφισμών 3.3.14. 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 ομομορφισμό δακτυλίων. Ο πυρήνας της ισούται προφανώς με

$$\begin{aligned} \mathrm{Ker}(f) &= \left\{a \in I + J \mid f(a) = 0_{((I+J)/I)\times((I+J)/J)}\right\} \\ &= \left\{a \in I + J \mid (a + I, a + J) = (I, J)\right\} \\ &= \left\{a \in I + J \mid a \in I, \; a \in J\right\} = I \cap J. \end{aligned}$$

Εν συνεχεία, θα δείξουμε ότι η f είναι επιρριπτική. Έστω τυχόν

$$(a + I, b + J) \in \left(\left(I + J\right)/I\right) \times \left(\left(I + J\right)/J\right).$$

Τότε τα a, b γράφονται ως αθροίσματα

$$a = u + v, \;\; b = w + z,$$

για κατάλληλα $u, w \in I$ και $v, z \in J$. Κατά συνέπειαν,

$$\begin{aligned} f(v) &= (v + I, v + J) = (v + I, 0_{I+J} + J), \\ f(w) &= (w + I, w + J) = (0_{I+J} + I, w + J), \end{aligned}$$

απ' όπου συμπεραίνουμε ότι

$$f(v + w) = f(v) + f(w) = (v + I, w + J) = (u + v + I, w + z + J) = (a + I, b + J),$$

δηλαδή ότι η f είναι επιμορφισμός 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 3.3.14 σε αμφότερους τους παράγοντες τού μετέχοντος καρτεσιανού γινομένου δακτυλίων. □

3.3.16 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 3.3.15 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,

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

3.3.17 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**.

3.3.18 Πόρισμα. *Εάν τα I, J είναι συμπρώτα ιδεώδη ενός δακτυλίου R, τότε*

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

3.3.19 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 $f = \varpi_2 \circ \varpi_1$, όπου $\varpi_1 : R \longrightarrow (R/I)$ και $\varpi_2 : R/I \longrightarrow (R/I) \,/\, (J/I)$ οι φυσικοί επιμορφισμοί, η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών 3.3.2,

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

Όμως

$$\begin{aligned}
\mathrm{Ker}(f) &= \left\{ a \in R \mid\ f(a) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \left\{ a \in R \mid\ \varpi_2(\varpi_1(a)) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \left\{ a \in R \mid\ \varpi_2(a+I) = 0_{(R/I)\,/\,(J/I)} \right\} \\
&= \{ a \in R \mid\ a+I \in \mathrm{Ker}\,(\varpi_2) \} \\
&= \{ a \in R \mid\ a+I \in (J/I) \} = J,
\end{aligned}$$

απ' όπου έπεται το ζητούμενο. □

3.3.20 Παράδειγμα. Εάν $R = \mathbb{Z}$ και $I = \langle 12 \rangle = 12\mathbb{Z} \subsetneqq J = \langle 3 \rangle = 3\mathbb{Z}$, τότε, επειδή το ιδεώδες $3\mathbb{Z}/12\mathbb{Z}$ τού δακτυλίου $\mathbb{Z}/12\mathbb{Z}$ περιέχει εκείνες τις κλάσεις υπολοίπων τού $\mathbb{Z}/12\mathbb{Z}$, οι εκπρόσωποι των οποίων ανήκουν στο $J = 3\mathbb{Z}$, ήτοι είναι πολλαπλάσια τού 3, έχουμε $J/I = \{I,\ 3+I,\ 6+I,\ 9+I\}$ και

$$(\mathbb{Z}/I) \,/\, (J/I) = \{ k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leq k \leq 11 \}\,.$$

Σημειωτέον ότι υπάρχουν πολλαπλές εμφανίσεις μεταξύ αυτών των δώδεκα στοιχείων, καθότι

$$\begin{aligned}
&(k_1+I)-(k_2+I) \in J/I \Longleftrightarrow (k_1-k_2)+I \in J/I \\
&\Longleftrightarrow 3 \mid k_1-k_2.
\end{aligned}$$

Ως εκ τούτου, ο δακτύλιος $(\mathbb{Z}/I) \,/\, (J/I)$ συνίσταται από ακριβώς τρεις διακεκριμένες κλάσεις ισοτιμίας:

$$(\mathbb{Z}/I) \,/\, (J/I) = \{ k + I + (J/I) \mid\ k \in \mathbb{Z},\ \ 0 \leq k \leq 2 \}\,.$$

Κατά το 1ο και το 3ο θεώρημα ισομορφισμών (βλ. 3.3.2 και 3.3.19),

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

3.4 ΕΦΑΡΜΟΓΗ: ΛΥΣΕΙΣ ΣΥΣΤΗΜΑΤΩΝ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Στην ενότητα 3.3 παρετέθησαν ορισμένα πρώτα παραδείγματα εφαρμογής των θεωρημάτων ισομορφισμών δακτυλίων (βλ. 3.3.3, 3.3.16 και 3.3.20). 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 επιλεγόμενο και *Κινέζικο θεώρημα*[3] ή *θεώρημα τού Νικομάχου τού Γερασηνού*[4], για το οποίο δίνουμε μια καθαρώς «δακτυλιοθεωρητική» απόδειξη (αν και στη γενίκευσή του 3.4.15 δεν παραλείπουμε και την παράθεση μιας πιο «στοιχειώδους» προσβάσεως).

► **Γραμμικές ισοτιμίες**. Έστω ότι ο m είναι ένας φυσικός αριθμός και οι a, b δυο ακέραιοι αριθμοί. Κάθε ισοτιμία τής μορφής

$$\boxed{ax \equiv b(\mathrm{mod}\, m),} \tag{3.8}$$

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 (3.8) όταν $ax_0 \equiv b(\mathrm{mod}\, m)$. Εν τοιαύτη περιπτώσει, *και οιοσδήποτε άλλος* εκπρόσωπος τής κλάσεως υπολοίπων $[x_0]_m$ τού x_0 επαληθεύει την (3.8). Πράγματι· εάν $y \in [x_0]_m$, τότε $[y]_m = [x_0]_m$, απ' όπου έπεται ότι $y \equiv x_0(\mathrm{mod}\, m)$, οπότε

$$ay \equiv ax_0 \equiv b(\mathrm{mod}\, m).$$

Ως εκ τούτου, όταν ομιλούμε για μια **λύση** $x_0 \in \mathbb{Z}$ **τής** (3.8) **κατά μόδιο** m, εννοούμε ολόκληρη[5] την κλάση $[x_0]_m$, όπου ο x_0 πληροί την (3.8). 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.

[3] Παρότι στη βιβλιογραφία είναι γνωστό ως *Chinese remainder theorem,* πιθανολογείται πως οι Κινέζοι μαθηματικοί τού 3ου μ.Χ. αιώνα, οι οποίοι έδωσαν μια πρακτική μέθοδο επιλύσεως ενός συστήματος τριών γραμμικών ισοτιμιών, είχαν λάβει γνώση τού έργου τού Νικομάχου τού Γερασηνού, αφού το εν λόγω σύστημα περιέχει τους ίδιους αριθμούς με εκείνους τού Νικομάχου! Η πρώτη ολοκληρωμένη απόδειξη τού θεωρήματος 3.4.10 οφείλεται στον L. Euler, ενώ μια νεότερη απόδειξη ανακαλύφθηκε (μάλλον ανεξαρτήτως) από τον C.-F. Gauss περί το έτος 1801.

[4] Ο φιλόσοφος και μαθηματικός *Νικόμαχος ο Γερασηνός* (από τα Γέρασα, μια αρχαιοελληνική πόλη στην Παλαιστίνη, 30 μίλια νοτιοανατολικά τής λίμνης Τιβεριάδος, ιδρυθείσα από τον Μ. Αλέξανδρο) θα πρέπει -εξ όσων γνωρίζουμενα έζησε σε κάποιο διάστημα μεταξύ τού μέσου τού 1ου και τού μέσου τού 2ου μ.Χ. αιώνα. Πέραν τής γνωστής του «Αριθμητικής Εισαγωγής» είχε συγγράψει και πολλά άλλα έργα, εκ των οποίων ελάχιστα τμήματα διεσώθησαν. Σε ένα όμως εξ αυτών παρατίθεται η λύση τού συστήματος των ισοτιμιών $x \equiv 2(\mathrm{mod}\, 3)$, $x \equiv 3(\mathrm{mod}\, 5)$ και $x \equiv 2(\mathrm{mod}\, 7)$. (Για να την προσδιορίσετε, εφαρμόστε τό 3.4.10!)

[5] Γι' αυτόν τον λόγο, δυο ακέραιες λύσεις x_1 και x_2 τής (3.8) λογίζονται ως *διαφορετικές* όταν $x_1 \not\equiv x_2(\mathrm{mod}\, m)$.

Σημειωτέον ότι υπάρχουν γραμμικές ισοτιμίες οι οποίες δεν δέχονται καμία ακεραία λύση, όπως π.χ. η $2x \equiv 3 (\mathrm{mod}\ 4)$, αφού για κάθε $k \in \mathbb{Z}$ ο ακέραιος $2k-3$ είναι περιττός και επομένως $4 \nmid 2k-3$. Η πρόταση που ακολουθεί μας γνωστοποιεί την ικανή και αναγκαία συνθήκη για την ύπαρξη ακεραίων λύσεων τής (3.8) 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* (3.8) *διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν* $\mu\kappa\delta\,(a,m) \mid b$. *Επιπροσθέτως, όταν* $\mu\kappa\delta\,(a,m) \mid b$, *η ισοτιμία* (3.8) *διαθέτει ακριβώς* $\mu\kappa\delta(a,m)$ *σαφώς διακεκριμένες λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής*

$$\boxed{x = x_0 + k\,\frac{m}{\mu\kappa\delta\,(a,m)}, \quad k \in \{0, 1, \ldots, \mu\kappa\delta\,(a,m) - 1\},} \tag{3.9}$$

όπου x_0 μια ειδική λύση τής (3.8).

ΑΠΟΔΕΙΞΗ. Εάν η (3.8) δέχεται μια λύση $x \in \mathbb{Z}$ κατά μόδιο m, τότε

$$ax \equiv b (\mathrm{mod}\ m) \Longrightarrow m \mid ax - b \Longrightarrow (\exists k \in \mathbb{Z} : b = ax - km)\,.$$

Επομένως,

$$\left.\begin{array}{r} \mu\kappa\delta\,(a,m) \mid a \\ \mu\kappa\delta\,(a,m) \mid m \end{array}\right\} \Longrightarrow \mu\kappa\delta\,(a,m) \mid ax - km\ (= b).$$

Και αντιστρόφως· εάν $\mu\kappa\delta(a,m) \mid b$, τότε $b = \mu\kappa\delta(a,m)\,b'$ για κάποιον $b' \in \mathbb{Z}$. Επειδή

$$\mu\kappa\delta\left(\tfrac{a}{\mu\kappa\delta(a,m)}, \tfrac{m}{\mu\kappa\delta(a,m)}\right) = 1 \Longrightarrow \left(\exists \kappa, \lambda \in \mathbb{Z} : \kappa\tfrac{a}{\mu\kappa\delta(a,m)} + \lambda\tfrac{m}{\mu\kappa\delta(a,m)} = 1\right),$$

λαμβάνουμε

$$b = \kappa\tfrac{ab}{\mu\kappa\delta(a,m)} + \lambda\tfrac{mb}{\mu\kappa\delta(a,m)} = a\,(\kappa b') + m\,(\lambda b') \Longrightarrow a\,(\kappa b') \equiv b (\mathrm{mod}\ m),$$

οπότε η κλάση ισοτιμίας τού $\kappa b'$ κατά μόδιο m είναι μια λύση τής (3.8).

Εν συνεχεία υποθέτουμε οτι το x_0 (ή, ακριβέστερα, η κλάση $[x_0]_m$) είναι μια παγιωμένη (ειδική) λύση τής (3.8). Προφανώς,

$$a\left(x_0 + k\frac{m}{\mu\kappa\delta\,(a,m)}\right) = ax_0 + \left(\frac{ak}{\mu\kappa\delta\,(a,m)}\right) m \equiv b (\mathrm{mod}\ m),$$

οπότε οι ακέραιοι (3.9) αποτελούν πράγματι λύσεις τής (3.8). Οι ακέραιοι αυτοί είναι ανά δύο ανισότιμοι κατά μόδιο m, καθότι για οιουσδήποτε ακεραίους αριθμούς $k, k' \in \{0, 1, \ldots, \mu\kappa\delta(a,m) - 1\}$ με $k \neq k'$, έχουμε

$$\left|\left(x_0 + \tfrac{mk}{\mu\kappa\delta(a,m)}\right) - \left(x_0 + \tfrac{mk'}{\mu\kappa\delta(a,m)}\right)\right| = |k - k'|\ \tfrac{m}{\mu\kappa\delta(a,m)} < m,$$

αφού $|k-k'|<$ μκδ(a,m) . Συνεπώς,

$$m \nmid \left(x_0+\tfrac{mk}{\text{μκδ}(a,m)}\right)-\left(x_0+\tfrac{mk'}{\text{μκδ}(a,m)}\right)$$
$$\Downarrow$$
$$\left(x_0+\tfrac{mk}{\text{μκδ}(a,m)}\right)\not\equiv\left(x_0+\tfrac{mk'}{\text{μκδ}(a,m)}\right)(\text{mod } m).$$

Απομένει λοιπόν να αποδειχθεί ότι και κάθε άλλη λύση $y\in\mathbb{Z}$ τής (3.8) είναι ισότιμη με κάποια εκ των (3.9) κατά μόδιο m. Επειδή

$$\left.\begin{array}{r} ax_0\equiv b(\text{mod } m)\\ ay\equiv b(\text{mod } m)\end{array}\right\}\Longrightarrow ax_0\equiv ay(\text{mod } m)\Longrightarrow m\mid a\,(y-x_0)\,,$$

συμπεραίνουμε ότι

$$\left.\begin{array}{l}\frac{m}{\text{μκδ}(a,m)}\mid\frac{a}{\text{μκδ}(a,m)}\,(y-x_0)\\ \text{μκδ}\left(\frac{a}{\text{μκδ}(a,m)},\frac{m}{\text{μκδ}(a,m)}\right)=1\end{array}\right\}\Longrightarrow\quad\begin{array}{c}\frac{m}{\text{μκδ}(a,m)}\mid y-x_0\\ \Downarrow\\ \left(\exists\nu\in\mathbb{Z}:y-x_0=\frac{m\nu}{\text{μκδ}(a,m)}\right).\end{array}$$

Διαιρώντας τον ν διά τού μκδ(a,m) λαμβάνουμε ένα μονοσημάντως ορισμένο ζεύγος $(q,r)\in\mathbb{Z}^2$ με

$$\nu=\text{μκδ}\,(a,m)\,q+r,\quad 0\le r\le\text{μκδ}\,(a,m)-1.$$

Ως εκ τούτου,

$$y-x_0=\tfrac{m(\text{μκδ}(a,m)q+r)}{\text{μκδ}(a,m)}=mq+\tfrac{rm}{\text{μκδ}(a,m)}\equiv\tfrac{rm}{\text{μκδ}(a,m)}(\text{mod } m),$$

οπότε $y\equiv x_0+r\frac{m}{\text{μκδ}(a,m)}(\text{mod } m),\forall r\in\{0,1,\dots,\text{μκδ}(a,m)-1\}$. □

3.4.2 Πόρισμα. *Δοθέντων ενός $m\in\mathbb{N}$ και δυο ακεραίων a,b, $a\neq 0$, η γραμμική ισοτιμία* (3.8) *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

$$a^{\varphi(m)}\equiv 1(\text{mod } m),$$

όπου φ η συνάρτηση φι τού Euler. Ως εκ τούτου, αρκεί να θέσουμε

$$\boxed{x_0 := a^{\varphi(m)-1}b,} \tag{3.10}$$

να εφαρμόσουμε τον γνωστό τύπο ευρέσεως τού $\varphi(m)$ 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 $\varphi(24) = (2^3 - 2^2)(3 - 1) = 8$. Κατά τον (3.10), 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 (3.8) 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* (3.8) *διαθέτει* μκδ(a, m) *λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής* (3.9), *όπου x_0 η μοναδική λύση κατά μόδιο $\frac{m}{\text{μκδ}(a,m)}$ τής*

$$\left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right) (\mathrm{mod}\ \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)). \tag{3.11}$$

ΑΠΟΔΕΙΞΗ. Θέτοντας $\widetilde{a} := \frac{a}{\text{μκδ}(a,m)}$, $\widetilde{b} := \frac{b}{\text{μκδ}(a,m)}$ και $\widetilde{m} := \frac{m}{\text{μκδ}(a,m)}$, έχουμε μκδ$(\widetilde{a}, \widetilde{m}) = 1$, καθώς και τις ακόλουθες αμφίπλευρες συνεπαγωγές:

$$\begin{aligned} ax \equiv b\ (\mathrm{mod}\ m) &\iff \text{μκδ}\,(a,m)\,\widetilde{a}x \equiv \text{μκδ}\,(a,m)\,\widetilde{b}\ (\mathrm{mod}\,\text{μκδ}\,(a,m)\,\widetilde{m}) \\ &\iff \widetilde{a}x \equiv \widetilde{b}\ (\mathrm{mod}\ \widetilde{m}) \\ &\iff \left(\tfrac{a}{\text{μκδ}(a,m)}\right) x \equiv \left(\tfrac{b}{\text{μκδ}(a,m)}\right)\ (\mathrm{mod}\ \ \left(\tfrac{m}{\text{μκδ}(a,m)}\right)), \end{aligned}$$

διότι μκδ$(a, m) \neq 0$, οπότε η (3.11) ισοδυναμεί με την (3.8). □

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 (3.10) θέτουμε

$$x_0 = 2^{\varphi(7)-1} = 2^5 = 32 \equiv 4 (\mathrm{mod}\, 7).$$

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 $m_1, \dots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \dots, a_k,\ b_1, \dots, b_k$, 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 $I_1, I_2, \dots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια, ώστε*

$$I_j + I_k = R,\ \forall\, (j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\quad j \neq k,$$

τότε

$$R = I_j + \bigcap_{1 \leq k \leq n,\ k \neq j} I_k,\quad \forall j \in \mathbb{N},\quad 1 \leq j \leq n.$$

ΑΠΟΔΕΙΞΗ. Θα κάνουμε χρήση μαθηματικής επαγωγής ως προς τον n. Για $n = 2$ ο ισχυρισμός είναι προφανώς αληθής. Υποθέτουμε λοιπόν ότι είναι αληθής και για κάποιον $n = l \geq 2$ και εξετάζουμε την περίπτωση όπου $n = l + 1$. Επειδή ο R είναι δακτύλιος με μοναδιαίο στοιχείο, έχουμε[6] $R = RR$. Κατά συνέπειαν, για κάθε $j \in \mathbb{N}$, $1 \leq j \leq l + 1$,

$$R = RR = \left(I_j + \bigcap_{1 \leq k \leq l,\ k \neq j} I_k \right) (I_j + I_{l+1}) \subseteq I_j + \bigcap_{1 \leq k \leq l+1,\ k \neq j} I_k,$$

με τη δεύτερη ισότητα ισχύουσα λόγω επαγωγικής υποθέσεως και την επακόλουθη εγκλειστική σχέση απορρέουσα από την πρόταση 2.4.5 (ii). Επειδή όμως το δεξιό μέλος εμπεριέχεται στον R, έχουμε $R = I_j + \bigcap_{1 \leq k \leq l+1,\ k \neq j} I_k$. □

3.4.8 Θεώρημα. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν $n \in \mathbb{N}$, $n \geq 2$, και εάν τα $I_1, I_2, \dots, I_n$ είναι ανά δύο συμπρώτα ιδεώδη τού R, ήτοι τέτοια ώστε*

$$I_j + I_k = R,\ \forall\, (j,k) \in \mathbb{N}^2,\ 1 \leq j,k \leq n,\quad j \neq k,$$

[6] Για δακτύλιους χωρίς μοναδιαίο κάτι τέτοιο δεν ισχύει εν γένει! Επί παραδείγματι, $(2\mathbb{Z})\,(2\mathbb{Z}) \subsetneq (2\mathbb{Z})$.

τότε έχουμε

$$\boxed{R/\bigcap_{j=1}^{n} I_j \cong (R/I_1) \times \cdots \times (R/I_n)}$$

ΠΡΩΤΗ ΑΠΟΔΕΙΞΗ. Για $n = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τού πορίσματος 3.3.18. Εάν υποτεθεί ότι για κάποιον φυσικό αριθμό $n \geq 3$ αυτός είναι αληθής για $n-1$ όρους, τότε μέσω μαθηματικής επαγωγής και εφαρμογής τού λήμματος 3.4.7 (για $j = n$) λαμβάνουμε

$$R/\bigcap_{j=1}^{n} I_j \cong R/(\bigcap_{j=1}^{n-1} I_j \cap I_n) \underset{3.3.18}{\cong} \left(R/\bigcap_{j=1}^{n-1} I_j \right) \times R/I_n$$
$$\underset{(\text{επαγ. υπ.})}{\cong} (R/I_1) \times \cdots \times (R/I_n)\,.$$

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ. Αυτή η απόδειξη είναι καθαρώς *κατασκευαστική*. Υποθέτοντας ότι ο $\varpi_j : R \longrightarrow R/I_j$ είναι ο επιμορφισμός των κλάσεων υπολοίπων τού R ως προς το I_j, για κάθε $j \in \{1, \ldots, n\}$, ορίζουμε την απεικόνιση

$$f : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$$

$$r \longmapsto f(r) := (\varpi_1(r), .., \varpi_n(r)) = (r + I_1, .., r + I_n)\,.$$

Η f είναι προφανώς ομομορφισμός δακτυλίων και $\mathrm{Ker}(f) = \bigcap_{j=1}^{n} I_j$. Θα δείξουμε ότι η f είναι και *επιριπτική*. Έστω $\mathbf{y} = (y_1, \ldots, y_n) \in (R/I_1) \times \cdots \times (R/I_n)$. Επειδή κάθε ϖ_j είναι επιριπτική απεικόνιση, υπάρχει $x_j \in R$, τέτοιο ώστε $\varpi_j(x_j) = y_j$. 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 $v_j \in I_k, \forall k \in \{1, \ldots, n\} \setminus \{j\}$, απ' όπου έπεται ότι

$$\varpi_k(v_j) = v_j + I_k = \begin{cases} 1_R + I_k, & \text{όταν } k = j, \\ I_k, & \text{όταν } k \neq j. \end{cases}$$

Συνεπώς,

$$\begin{aligned} f\left(\sum_{j=1}^{n} x_j v_j\right) &= \left(\varpi_1(\sum_{j=1}^{n} x_j v_j), \ldots, \varpi_n(\sum_{j=1}^{n} x_j v_j)\right) \\ &= (\varpi_1(x_1), \ldots, \varpi_n(x_n)) = \mathbf{y}, \end{aligned} \tag{3.12}$$

και η f είναι όντως επιρριπτική. Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.2, ούτως ώστε να εισπράξουμε έναν «απτό» ισομορφισμό

$$\begin{array}{rcl} R/\bigcap_{j=1}^{n} I_j & \xrightarrow{\cong} & (R/I_1)\times\cdots\times(R/I_n) \\ r+\bigcap_{j=1}^{n} I_j & \longmapsto & f(r)=(r+I_1,\ldots,r+I_n) \end{array} \tag{3.13}$$

μεταξύ των δύο θεωρηθέντων πηλικοδακτυλίων. □

3.4.9 Πόρισμα. *Έστω n ένας φυσικός αριθμός ≥ 2 και έστω*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

η παράσταση τού n ως γινομένου διακεκριμένων πρώτων αριθμών $p_1, p_2, \ldots, p_k$, υψωμένων σε κατάλληλες δυνάμεις $\alpha_1, \alpha_2, \ldots, \alpha_k$. Τότε έχουμε

$$\boxed{\mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}/(p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times \mathbb{Z}/(p_k^{\alpha_k}\mathbb{Z}).}$$

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,

$$\left.\begin{array}{r} p_j^{\alpha_j} \,|\, x, \quad \forall j \in \{1, \ldots, k\} \\ p_1, p_2, \ldots, p_k \text{ διακεκριμένοι} \end{array}\right\} \Longrightarrow n = \prod_{j=1}^{k} p_j^{\alpha_j} \,\Big|\, x \Longrightarrow x \in \langle n \rangle = n\mathbb{Z}.$$

Αρκεί λοιπόν να εφαρμόσουμε το θεώρημα 3.4.8. □

3.4.10 Πόρισμα. (Κινέζικο Θεώρημα ή Θεώρημα τού Νικομάχου τού Γερασηνού) *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ και k ακεραίων αριθμών $b_1, \ldots, b_k$, για τους οποίους ισχύει*

$$\text{μκδ}\,(m_j, m_l) = 1, \ \forall\,(j,l) \in \mathbb{N}^2, \ 1 \leq j, l \leq n, \quad j \neq l,$$

το σύστημα των γραμμικών ισοτιμιών

$$\left\{\begin{array}{c} x \equiv b_1 \,(\mathrm{mod}\ \ m_1) \\ \vdots \\ x \equiv b_k \,(\mathrm{mod}\ \ m_k) \end{array}\right\} \tag{3.14}$$

είναι επιλύσιμο. Μάλιστα, εάν το x_0 είναι μια λύση τού (3.14)*, τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο $m := \prod_{j=1}^{k} m_j$. *Ως εκ τούτου, το σύνολο των λύσεων τού συστήματος* (3.14) *είναι η κλάση υπολοίπων*[7]

$$x_0 + m\mathbb{Z} \ \ (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

ΑΠΟΔΕΙΞΗ. Εάν για κάθε φυσικό αριθμό n και κάθε πρώτο αριθμό p ορίσουμε ως

$$\boldsymbol{\nu}_p\,(n) := \left\{\begin{array}{l} \text{τον εκθέτη τής μεγίστης δυνατής} \\ \text{δυνάμεως τού } p \text{ που διαιρεί τον } n \end{array}\right\} \in \mathbb{N}_0,$$

τότε, σύμφωνα με το πόρισμα 3.4.9,

$$\mathbb{Z}/\,(m\mathbb{Z}) \cong \prod_{p \text{ πρώτος},\ p|m_1} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_1)}\mathbb{Z}) \times \cdots \times \prod_{p \text{ πρώτος},\ p|m_k} \mathbb{Z}/(p^{\boldsymbol{\nu}_p(m_k)}\mathbb{Z}),$$

και επειδή

$$m_j = \prod_{p \text{ πρώτος},\ p|m_j} p^{\boldsymbol{\nu}_p(m_j)}, \ \ \forall j \in \{1, \ldots, k\},$$

[7] Εν προκειμένω, μπορούμε να *ταυτίζουμε* την $x_0 + m\mathbb{Z} \ \ \in \mathbb{Z}/\,(m\mathbb{Z})$ με την κλάση ισοτιμίας $[x_0]_m \in \mathbb{Z}_m$ μέσω τού ισομορφισμού (3.5).

συμπεραίνουμε ότι

$$\mathbb{Z}/\left(m\mathbb{Z}\right) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}).$$

Εάν, μάλιστα, λάβει κανείς υπ' όψιν το 3.4.9 και τον (3.13), ο *τύπος ορισμού* αυτού τού ισομορφισμού είναι γνωστός, ήτοι ο

$$\mathbb{Z}/\left(m\mathbb{Z}\right) \ni \lambda + m\mathbb{Z} \longmapsto (\lambda + m_1\mathbb{Z}, \ldots, \lambda + m_k\mathbb{Z}) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z}). \quad (3.15)$$

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 (3.15), 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 (3.14) κατά μόδιο m. □

3.4.11 Σημείωση. Για την εύρεση μιας λύσεως x_0 τού συστήματος (3.14) αρκεί, για κάθε δείκτη $j \in \{1, ..., k\}$, να προσδιορισθούν

$$u_j \in \langle m_j \rangle\,,\ \ v_j \in \left\langle m'_j \right\rangle = \bigcap_{1 \le l \le k,\ l \ne j} \langle m_l \rangle\,,$$

όπου

$$m'_j := \prod_{1 \le l \le k,\ l \ne j} m_l,$$

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 $z_j := {m'_j}^{\varphi(m_j)-1}$. Από τα δεδομένα μας (βλ. (3.12), (3.13) και (3.15)) έπεται ότι το

$$\boxed{x_0 = \sum_{j=1}^{k} \frac{b_j z_j m}{m_j} = \sum_{j=1}^{k} b_j m'_j z_j = \sum_{j=1}^{k} b_j {m'_j}^{\varphi(m_j)}} \quad (3.16)$$

-ανηγμένο κατά μόδιο m- είναι μια λύση τού συστήματος ισοτιμιών (3.14), ενώ κάθε άλλη λύση του προκύπτει κατόπιν αθροίσεως (σε αυτό) ενός ακεραίου πολλαπλασίου τού m.

3.4.12 Παράδειγμα. Το σύνολο των λύσεων τού συστήματος γραμμικών ισοτιμιών

$$\left\{ \begin{array}{l} x \equiv 1 \,(\mathrm{mod}\ 3) \\ x \equiv 2 \,(\mathrm{mod}\ 4) \\ x \equiv 3 \,(\mathrm{mod}\ 5) \end{array} \right\}$$

είναι η κλάση υπολοίπων $58 + 60\mathbb{Z}$ $(\in \mathbb{Z}/60\mathbb{Z})$, διότι (κατά τον τύπο (3.16))

$$\begin{aligned} x_0 &= \left(1 \cdot 20^{\varphi(3)} + 2 \cdot 15^{\varphi(4)} + 3 \cdot 12^{\varphi(5)}\right) \\ &= 1 \cdot 20^2 + 2 \cdot 15^2 + 3 \cdot 12^4 \\ &= 1 \cdot 400 + 2 \cdot 225 + 3 \cdot 20\,736 \\ &= 63\,058 \equiv 58 \,(\mathrm{mod}\ 60)\,. \end{aligned}$$

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

$$\left.\begin{array}{l} m_1 \mid x - b_1 \\ m_2 \mid x - b_2 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} \text{μκδ}\,(m_1, m_2) \mid x - b_1 \\ \text{μκδ}\,(m_1, m_2) \mid x - b_2 \end{array}\right\} \Longrightarrow \text{μκδ}\,(m_1, m_2) \mid x - b_1 - (x - b_2)\,.$$

Και αντιστρόφως· εάν $d := \text{μκδ}(m_1, m_2)$ και $d \mid b_2 - b_1$, γράφοντας τον d ως ακέραιο γραμμικό συνδυασμό

$$d = k_1 m_1 + k_2 m_2, \quad k_1, k_2 \in \mathbb{Z},$$

και θέτοντας $\nu := \frac{k_1(b_2 - b_1)}{d}$, λαμβάνουμε

$$m_1 \nu \equiv (d - k_2 m_2)\,\tfrac{(b_2 - b_1)}{d} \equiv b_2 - b_1 \,(\mathrm{mod}\, m_2)\,,$$

οπότε για τον ακέραιο αριθμό $x := b_1 + m_1\nu$ ισχύουν οι ισοτιμίες $x \equiv b_1 \,(\mathrm{mod}\ m_1)$ και $x \equiv b_1 + (b_2 - b_1) \equiv b_2 \,(\mathrm{mod}\ m_2)$. □

3.4.14 Λήμμα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \ldots, m_k$ έχουμε*

$$\text{μκδ}\,(\text{εκπ}\,(m_1, \ldots, m_{k-1}), m_k) = \text{εκπ}\,(\text{μκδ}\,(m_1, m_k), \ldots, \text{μκδ}\,(m_{k-1}, m_k))$$

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*

$$\left\{ \begin{array}{c} x \equiv b_1 \,(\mathrm{mod}\ m_1) \\ \vdots \\ x \equiv b_k \,(\mathrm{mod}\ m_k) \end{array} \right\} \tag{3.17}$$

είναι επιλύσιμο εάν και μόνον εάν

$$\text{μκδ}\,(m_j, m_l) \mid b_j - b_l, \quad \forall\,(j,l) \in \mathbb{N}^2,\ 1 \leq j, l \leq k, \quad j \neq l. \tag{3.18}$$

Μάλιστα, εάν το x_0 είναι μια λύση τού (3.17)*, τότε αυτή είναι* μονοσημάντως ορισμένη κατά μόδιο

$$m := \text{εκπ}\,(m_1, m_2, ..., m_k)\,.$$

Ως εκ τούτου, όταν ικανοποιούνται οι συνθήκες (3.18)*, το σύνολο των λύσεων τού συστήματος* (3.17) *είναι η κλάση υπολοίπων*

$$x_0 + m\mathbb{Z} \quad (\in \mathbb{Z}/\,(m\mathbb{Z})).$$

ΑΠΟΔΕΙΞΗ. (i) Έστω x_0 είναι μια λύση τού (3.17). Τότε για κάθε $j, l \in \{1, \ldots, k\}$ με $j \neq l$ έχουμε

$$\left.\begin{array}{c} x_0 \equiv b_j \,(\mathrm{mod}\ m_j) \\ x_0 \equiv b_l \,(\mathrm{mod}\ m_l) \end{array}\right\} \Longrightarrow \left.\begin{array}{c} m_j \mid x_0 - b_j \\ m_l \mid x_0 - b_l \end{array}\right\} \Longrightarrow \left.\begin{array}{c} \text{μκδ}\,(m_j, m_l) \mid x_0 - b_j \\ \text{μκδ}\,(m_j, m_l) \mid x_0 - b_l \end{array}\right\} \Longrightarrow (3.18).$$

Και αντιστρόφως· ας υποθέσουμε την ισχύ των συνθηκών (3.18).

Εργαζόμενοι επαγωγικώς θα κατασκευάσουμε για κάθε $j \in \{1, \ldots, k\}$ έναν ακέραιο αριθμό y_j, ούτως ώστε να ισχύουν οι ισοτιμίες

$$\left\{ \begin{array}{c} y_j \equiv b_1 \,(\mathrm{mod}\ m_1) \\ \vdots \\ y_j \equiv b_j \,(\mathrm{mod}\ m_j) \end{array} \right\}.$$

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

$$y_j \equiv b_l \,(\mathrm{mod}\ m_l)\,, \quad \forall l \in \{1, \ldots, j\},$$

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,

$$\text{μκδ}\,(m_l, m_{j+1}) \mid b_l - b_{j+1},\ \forall l \in \{1, \dots, j\}.$$

Άρα

$$\text{μκδ}\,(m_l, m_{j+1}) \mid (y_j - b_l) - (b_l - b_{j+1}) = y_j - b_{j+1},\ \forall l \in \{1, \dots, j\}$$

και, ως εκ τούτου,

$$\text{εκπ}\,(\text{μκδ}\,(m_1, m_{j+1}), \dots, \text{μκδ}\,(m_j, m_{j+1})) \mid y_j - b_{j+1}.$$

Εφαρμόζοντας λοιπόν το λήμμα 3.4.14 συμπεραίνουμε ότι

$$\text{μκδ}\,(\text{εκπ}\,(m_1, \dots, m_j), m_{j+1}) \mid y_j - b_{j+1}.$$

Κατά συνέπειαν, βάσει τού λήμματος 3.4.13 υπάρχει ένας $y_{j+1} \in \mathbb{Z}$, τέτοιος ώστε

$$y_{j+1} \equiv y_j \,(\text{mod } \text{εκπ}\,(m_1, \dots, m_j)) \qquad y_{j+1} \equiv b_{j+1} \,(\text{mod } m_{j+1}),$$

οπότε

$$[m_l \mid \text{εκπ}\,(m_1, .., m_j),\ \forall l \in \{1, .., j\}] \Longrightarrow y_{j+1} \equiv y_j \equiv b_l \,(\text{mod } m_l), \forall l \in \{1, .., j\}.$$

(ii) Έστω τώρα $m := \text{εκπ}(m_1, m_2, ..., m_k)$ και έστω x_0 ένας εκπρόσωπος τής κλάσεως υπολοίπων $[y_k]_m$ (όπου $0 \leq x_0 < m$). Εάν ο x είναι ένας ακέραιος αριθμός, ο οποίος πληροί τις k ισοτιμίες (3.17), τότε έχουμε

$$[x \equiv b_\ell \equiv x_0 \,(\text{mod } m_\ell), \forall \ell \in \{1, \dots, k\}],$$

οπότε

$$[m_\ell \mid x_0 - x,\ \forall \ell \in \{1, \dots, k\}] \Longrightarrow m \mid x_0 - x \Longrightarrow x_0 - x \in m\mathbb{Z}.$$

Και αντιστρόφως· εάν $x \in \mathbb{Z}$ και $x \equiv x_0 \,(\text{mod } m)$, τότε έχουμε προφανώς για κάθε $\ell \in \{1, \dots, k\}$: $x \equiv b_\ell \equiv x_0 \,(\text{mod } m_\ell)$. □

3.4.16 Θεώρημα. *Έστω $k \in \mathbb{N}$, $k \geq 2$. Δοθέντων k φυσικών αριθμών $m_1, \dots, m_k$ και $2k$ ακεραίων αριθμών $a_1, \dots, a_k,\ b_1, \dots, b_k$, το σύστημα των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} a_1 x \equiv b_1 \,(\text{mod } m_1) \\ \vdots \\ a_k x \equiv b_k \,(\text{mod } m_k) \end{array} \right\} \tag{3.19}$$

δεν είναι επιλύσιμο εάν δεν ικανοποιούνται ταυτοχρόνως οι συνθήκες

$$\text{μκδ}\,(a_j, m_j) \mid b_j, \quad \forall j \in \{1, ..., k\}. \tag{3.20}$$

Από την άλλη μεριά, όταν οι συνθήκες (3.20) *ικανοποιούνται, το σύνολο των λύσεων τού συστήματος* (3.19) *ταυτίζεται με το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών*

$$\left\{ \begin{array}{c} x \equiv c_1 \,(\mathrm{mod}\ m_1^\star) \\ \vdots \\ x \equiv c_k \,(\mathrm{mod}\ m_k^\star) \end{array} \right\} \tag{3.21}$$

όπου

$$c_j := \left(a_j^\star\right)^{\varphi\left(m_j^\star\right)-1}\ b_j^\star$$

και

$$a_j^\star := \frac{a_j}{\text{μκδ}\,(a_j, m_j)}, \quad b_j^\star := \frac{b_j}{\text{μκδ}\,(a_j, m_j)}, \quad m_j^\star := \frac{m_j}{\text{μκδ}\,(a_j, m_j)},$$

για κάθε $j \in \{1, ..., k\}$ *και* φ *η συνάρτηση τού Euler.*

ΑΠΟΔΕΙΞΗ. Για να υπάρχουν κοινές λύσεις τού συστήματος (3.19) 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 (3.20) ικανοποιούνται, εφαρμόζουμε το πόρισμα 3.4.5 για κάθε μία εκ των αρχικών ισοτιμιών και συμπεραίνουμε ότι το (3.19) ισοδυναμεί με το σύστημα

$$\left\{ \begin{array}{c} a_1^\star x \equiv b_1^\star \,(\mathrm{mod}\ m_1^\star) \\ \vdots \\ a_k^\star x \equiv b_k^\star \,(\mathrm{mod}\ m_k^\star) \end{array} \right\} \tag{3.22}$$

Επειδή μκδ$(a_j^\star, m_j^\star) = 1$, η γραμμική ισοτιμία $a_j^\star x \equiv b_j^\star \left(\mathrm{mod}\ m_j^\star\right)$ διαθέτει μοναδική λύση κατά μόδιο $m_j^\star$, ήτοι την $x \equiv c_j (\mathrm{mod}\ m_j^\star)$ (βλ. 3.4.3), οπότε το σύνολο των λύσεων τού συστήματος των γραμμικών ισοτιμιών (3.22) ταυτίζεται με το σύνολο των λύσεων τού συστήματος (3.21). □

3.4.17 Παρατήρηση. Προφανώς, το πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.19) ανάγεται στο πρόβλημα τής ευρέσεως τού συνόλου των λύσεων τού (3.21), ήτοι ενός συστήματος τού τύπου (3.17), οπότε αντιμετωπίζεται βάσει των όσων ελέχθησαν στο θεώρημα 3.4.15.

3.4.18 Παράδειγμα. Ας θεωρήσουμε το ακόλουθο σύστημα τριών γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{l} 2x \equiv 4 \,(\mathrm{mod}\ 8) \\ 6x \equiv 12 \,(\mathrm{mod}\ 9) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\}.$$

Επειδή μκδ$(2,8) = 2 \mid 4$, μκδ$(6,9) = 3 \mid 12$ και μκδ$(1,12) = 1 \mid 14$, αυτό είναι ισοδύναμο με το

$$\left\{ \begin{array}{l} x \equiv 2 \,(\mathrm{mod}\ 4) \\ 2x \equiv 4 \,(\mathrm{mod}\ 3) \\ x \equiv 14 \,(\mathrm{mod}\ 12) \end{array} \right\}.$$

Η δεύτερη ισοτιμία έχει ως λύση της την κλάση υπολοίπων $2 + 3\mathbb{Z}$ $(\in \mathbb{Z}/3\mathbb{Z})$, διότι $2^{\varphi(3)-1} \cdot 4 = 8 \equiv 2 \,(\mathrm{mod}\ 3)$. 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 (3.16),

$$x_0 = 2 \cdot 3^{\varphi(4)} + 2 \cdot 4^{\varphi(3)} = 50 \equiv 2 \,(\mathrm{mod}\ 12)\,,$$

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 $R \times (R \setminus \{0_R\})$ 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

$$ab = ba \Rightarrow (a,b) \sim (a,b)\,, \ \ \forall (a,b) \in R \times (R \setminus \{0_R\})\,,$$

συμμετρική, διότι για οιαδήποτε ζεύγη $(a,b), (c,d) \in R \times (R \setminus \{0_R\})$ έχουμε

$$(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)\,,$$

και, τέλος, *μεταβατική*, αφού για οιαδήποτε $(a,b), (a',b'), (a'',b'') \in R \times (R \setminus \{0_R\})$ 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

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

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

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

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

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

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

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

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

Πράγματι· επειδή εξ υποθέσεως

$$\left.\begin{matrix}(a,b)\sim(a',b')\\(c,d)\sim(c',d')\end{matrix}\right\}\Longrightarrow\left.\begin{matrix}ab'=ba'\\cd'=dc'\end{matrix}\right\}\Longrightarrow\left.\begin{matrix}ab'dd'=ba'dd'\\cd'bb'=dc'bb'\end{matrix}\right\},$$

(κατόπιν προσθέσεως κατά μέλη) έπεται ότι

$$ab'dd'+cd'bb'=ba'dd'+dc'bb'\Longrightarrow(ad+cb)\,b'd'=(a'd'+c'b')\,bd,$$

ήτοι ότι

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

Εξάλλου, πολλαπλασιασμός κατά μέλη μάς οδηγεί στην ισότητα $ab'cd'=ba'dc'$, απ' όπου λαμβάνουμε

$$(ac)\,(b'd')=(bd)\,(a'c')\Longrightarrow\tfrac{ac}{bd}=\tfrac{a'c'}{b'd'},$$

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

3.5.5 Θεώρημα. *Το σύνολο* $\mathbf{Fr}(R)$ *των κλασμάτων μιας ακεραίας περιοχής* R *αποτελεί ένα σώμα ως προς τις ως άνω ορισθείσες πράξεις προσθέσεως και πολλαπλασιασμού.* (*Γι' αυτόν τον λόγο το* $\mathbf{Fr}(R)$ *ονομάζεται* ***σώμα κλασμάτων*** *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

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

για οιαδήποτε κλάσματα $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in\mathbf{Fr}(R)$.

(ii) Το *μηδενικό στοιχείο* (= ουδέτερο στοιχείο ως προς την "+") τού $\mathbf{Fr}(R)$ είναι το[8] $0_{\mathbf{Fr}(R)} := \frac{0_R}{1_R}$, διότι για κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\frac{a}{b} + \frac{0_R}{1_R} = \frac{(a\cdot 1_R)+(b\cdot 0_R)}{b\cdot 1_R} = \frac{a}{b} = \frac{(b_R\cdot b)+(1_R\cdot a)}{1_R\cdot b} = \frac{0_R}{1_R} + \frac{a}{b}.$$

(iii) Κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ έχει το κλάσμα $\frac{-a}{b}$ ως *αντίθετό του* ως προς την "+", καθότι

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-a)b}{b^2} = \frac{(a+(-a))b}{b^2} = \frac{a+(-a)}{b} = \frac{0_R}{b} = \frac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}$$

και

$$\frac{-a}{b} + \frac{a}{b} = \frac{(-a)b+ab}{b^2} = \frac{((-a)+a)b}{b^2} = \frac{(-a)+a}{b} = \frac{0_R}{b} = \frac{0_R}{1_R} = 0_{\mathbf{Fr}(R)}.$$

(iv) Η "$\cdot$" είναι *προσεταιριστική και μεταθετική*, διότι

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f} = \left(\frac{ac}{bd}\right)\cdot\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b}\cdot\left(\frac{ce}{df}\right) = \frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)$$

και

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\cdot\frac{a}{b}$$

για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$.

(v) Η "$\cdot$" είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "+". Επειδή η "$\cdot$" είναι μεταθετική, αρκεί προς τούτο να ελεγχθεί η επιμεριστικότητα μόνον εκ δεξιών. Για οιαδήποτε κλάσματα $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f} &= \left(\frac{ad+cb}{bd}\right)\cdot\frac{e}{f} = \frac{(ad+cb)e}{(bd)f} = \frac{ade+cbe}{bdf} = \frac{ade}{bdf} + \frac{cbe}{bdf}\\ &= \frac{ae}{bf} + \frac{ce}{df} = \left(\frac{a}{b}\cdot\frac{e}{f}\right) + \left(\frac{c}{d}\cdot\frac{e}{f}\right).\end{aligned}$$

(vi) Το $1_{\mathbf{Fr}(R)} := \frac{1_R}{1_R}$ είναι *μοναδιαίο στοιχείο*[9] (= ουδέτερο στοιχείο ως προς την "$\cdot$") τού $\mathbf{Fr}(R)$, διότι για κάθε κλάσμα $\frac{a}{b} \in \mathbf{Fr}(R)$ ισχύουν οι ισότητες

$$\frac{a}{b}\cdot 1_{\mathbf{Fr}(R)} = \frac{a}{b}\cdot\frac{1_R}{1_R} = \frac{a\cdot 1_R}{b\cdot 1_R} = \frac{a}{b} = \frac{1_R\cdot a}{1_R\cdot b} = \frac{1_R}{1_R}\cdot\frac{a}{b} = 1_{\mathbf{Fr}(R)}\cdot\frac{a}{b}.$$

(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 $\frac{a}{b} \in \mathbf{Fr}(R)\setminus\{0_{\mathbf{Fr}(R)}\}$ είναι αντιστρέψιμο. Επειδή από τη συνθήκη $\frac{a}{b} \neq \frac{0_R}{1_R}$ προκύπτει ότι

$$a = a\cdot 1_R \neq 0_R\cdot b = 0_R \Longrightarrow \frac{b}{a} \in \mathbf{Fr}(R),$$

[8] Σημειωτέον ότι *για κάθε* $b \in R\setminus\{0_R\}$ έχουμε $\frac{0_R}{b} = \frac{0_R}{1_R}$.

[9] Σημειωτέον ότι *για κάθε* $c \in R\setminus\{0_R\}$ έχουμε $\frac{c}{c} = 1_{\mathbf{Fr}(R)}$.

εκ των ισοτήτων

$$\begin{aligned} \tfrac{a}{b}\cdot\tfrac{b}{a} &= \tfrac{ab}{ba}=\tfrac{ab}{ab}=\tfrac{1_R}{1_R} \\ &= 1_{\mathbf{Fr}(R)}=\tfrac{ba}{ba}=\tfrac{ba}{ab}=\tfrac{b}{a}\cdot\tfrac{a}{b} \end{aligned}$$

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 μιας μεταβλητής** 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 **μεταβλητών** $\mathsf{X}_1,..,\mathsf{X}_n$ **υπεράνω τού** K.

(iii) Εντός τής ακεραίας περιοχής $\mathbb{C}[\![\mathsf{Z}]\!]$ των επίτυπων δυναμοσειρών μιας μιγαδικής μεταβλητής Z (ήτοι μιας μεταβλητής Z υπεράνω τού $\mathbb{C}$) ορίζεται η υποπεριοχή

$$\mathbb{C}\{\mathsf{Z}\}:=\left\{\sum_{i=0}^{\infty}a_i\mathsf{Z}^i\in\mathbb{C}[\![\mathsf{Z}]\!]\;\middle|\;\sum_{i=0}^{\infty}a_iz^i\text{ συγκλίνουσα για κάθε }z\in\mathbb{C}\right\}.$$

Ως γνωστόν[10], $\mathbb{C}\{\mathsf{Z}\}=\mathcal{O}(\mathbb{C})$, όπου

$$\boxed{\mathcal{O}(\mathbb{C}):=\{\text{συναρτήσεις }f:\mathbb{C}\longrightarrow\mathbb{C}\,|\,f\text{ ολόμορφη}\}}$$

η ακεραία περιοχή των λεγομένων **ακεραίων συναρτήσεων** μιας μιγαδικής μεταβλητής. Το σώμα κλασμάτων της

$$\boxed{\mathcal{M}(\mathbb{C}):=\mathbf{Fr}(\mathcal{O}(\mathbb{C}))}$$

καλείται **σώμα των μερομόρφων συναρτήσεων** επί τού $\mathbb{C}$ (και τα στοιχεία του **μερόμορφες συναρτήσεις** επί τού $\mathbb{C}$, τις οποίες συναντούμε συχνά στο μάθημα τής Μιγαδικής Αναλύσεως).

(iv) Έστω R μια ακεραία περιοχή. Τότε

$$\boxed{\mathbf{Fr}(R\,[\mathsf{X}])=\mathbf{Fr}(R)(\mathsf{X})\;(:=\mathbf{Fr}(\mathbf{Fr}(R)[\mathsf{X}])),}$$

[10]Κάθε *ολόμορφη συνάρτηση* $f:\mathbb{C}\longrightarrow\mathbb{C}$ (ήτοι κάθε συνάρτηση $f:\mathbb{C}\longrightarrow\mathbb{C}$ διαθέτουσα μιγαδική παράγωγο σε κάθε σημείο τού $\mathbb{C}$) είναι *παραστάσιμη ως συγκλίνουσα δυναμοσειρά*.

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

$$\begin{aligned} \mathbf{Fr}(R)(\mathsf{X}) &= \left\{ \tfrac{r_0 + r_1\mathsf{X} + \cdots + r_n\mathsf{X}^n}{s_0 + s_1\mathsf{X} + \cdots + s_m\mathsf{X}^m} \,\middle|\, \begin{array}{c} m, n \in \mathbb{N}_0, r_0, \ldots, r_n, s_0, \ldots, s_m \in \mathbf{Fr}(R) \\ \text{με } \ s_j \neq 0_{\mathbf{Fr}(R)} \text{ για κάποιον } \ j \in \{0, \ldots, m\} \end{array} \right\} \\ &= \left\{ \tfrac{\frac{a_0}{b_0} + \left(\frac{a_1}{b_1}\right)\mathsf{X} + \cdots + \left(\frac{a_n}{b_n}\right)\mathsf{X}^n}{\frac{c_0}{d_0} + \left(\frac{c_1}{d_1}\right)\mathsf{X} + \cdots + \left(\frac{c_m}{d_m}\right)\mathsf{X}^m} \,\middle|\, \begin{array}{c} r_i = \frac{a_i}{b_i},\ s_j = \frac{c_j}{d_j}, \\ \text{όπου } (a_i, b_i), (c_j, d_j) \in R \times (R \smallsetminus \{0_R\}), \\ \forall (i,j) \in \{0, \ldots, n\} \times \{0, \ldots, m\} \end{array} \right\} \\ &= \mathbf{Fr}(R[\mathsf{X}]), \end{aligned}$$

με την τελευταία ισότητα προκύπτουσα ύστερα από απαλοιφή παρονομαστών.

(v) Εάν το K είναι ένα σώμα, τότε το σώμα των κλασμάτων τής ακεραίας περιοχής $K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας μεταβλητής X με συντελεστές ειλημμένους από το K συμβολίζεται συντόμως ως ακολούθως:

$$\boxed{K(\!(\mathsf{X})\!) := \mathbf{Fr}(K[\![\mathsf{X}]\!]).}$$

Σημειωτέον ότι

$$\boxed{K(\!(\mathsf{X})\!) = \mathbf{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]}$$

(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,

$$\begin{aligned} K(\!(\mathsf{X})\!) &= \left\{ \frac{\sum_{i=0}^{\infty} c_i \mathsf{X}^i}{\mathsf{X}^l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \left\{ \sum_{i=0}^{l-1} c_i \mathsf{X}^{i-l} + \sum_{i=l}^{\infty} c_i \mathsf{X}^{i-l} \,\middle|\, c_i \in K,\ \forall i \in \mathbb{N}_0,\ \ l \in \mathbb{N} \right\} \\ &= \mathrm{Laur}_K[\![\mathsf{X}^{\pm 1}]\!]. \end{aligned}$$

3.5.7 Πρόταση. *Κάθε ακεραία περιοχή εμφυτεύεται στο σώμα των κλασμάτων της.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα ακεραία περιοχή. Τότε ο ομομορφισμός

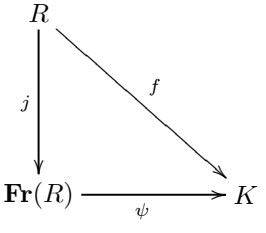
$$j : R \longrightarrow \mathbf{Fr}(R), \quad a \longmapsto j(a) := \tfrac{a}{1_R}, \tag{3.23}$$

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*

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

ο οποίος καθιστά το διάγραμμα



μεταθετικό (ήτοι $f = \psi \circ j$), όπου j ο μονομορφισμός (3.23).

ΑΠΟΔΕΙΞΗ. Ορίζουμε την $\psi : \mathbf{Fr}(R) \longrightarrow K$ μέσω τού τύπου

$$\psi(\tfrac{a}{b}) := f\,(a)\, f\,(b)^{-1}, \ \ \forall \tfrac{a}{b} \in \mathbf{Fr}(R).$$

Η ψ 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

$$f(b), f(b') \in \mathbf{Fr}(R)^{\times} \Rightarrow \psi(\tfrac{a}{b}) := f(a)\, f(b)^{-1} = f(a')\, f(b')^{-1} =: \psi(\tfrac{a'}{b'}).$$

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

$$\begin{aligned} \psi(\tfrac{a}{b} + \tfrac{c}{d}) &= \psi(\tfrac{ad+cb}{bd}) = f(ad+cb)\, f(bd)^{-1} \\ &= (f(a)f(d) + f(c)f(b))\, f(b)f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)\, f(d)^{-1} = \psi(\tfrac{a}{b}) + \psi(\tfrac{c}{d}) \end{aligned}$$

και

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

Η ψ είναι *ενριπτική*, διότι εάν $\frac{a}{b}, \frac{c}{d} \in \mathbf{Fr}(R)$ με $\psi(\frac{a}{b}) = \psi(\frac{c}{d})$, τότε

$$f(a)\, f(b)^{-1} = f(c)\, f(d)^{-1} \Rightarrow f(a)\, f(d) = f(b)\, f(c),$$

ήτοι

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

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

$$(\psi \circ j)(a) = \psi(j(a)) = \psi(\tfrac{a}{1_R}) = f(a)f(1_R)^{-1} = f(a) \cdot 1_K = f(a)$$

για κάθε $a \in R$, οπότε $f = \psi \circ j$. Τέλος, εάν υποτεθεί ότι υφίσταται κάποιος μονομορφισμός $\psi' : \mathbf{Fr}(R) \longrightarrow K$ για τον οποίο ισχύει η ισότητα $f = \psi' \circ j$, τότε για κάθε $\frac{a}{b} \in \mathbf{Fr}(R)$ έχουμε

$$\begin{aligned} \psi'(\tfrac{a}{b}) &= \psi'(j(a)j(b^{-1})) = \psi'(j(ab^{-1})) = (\psi' \circ j)(ab^{-1}) \\ &= f(ab^{-1}) = f(a)f(b)^{-1} = \psi(\tfrac{a}{b}), \end{aligned}$$

απ' όπου έπεται ότι $\psi' = \psi$. □

3.5.9 Πόρισμα. *Εάν η R είναι μια ακεραία περιοχή περιεχόμενη σε ένα σώμα K, τότε το*

$$\overline{R} := \left\{ ab^{-1} \middle| \, (a,b) \in R \times (R \setminus \{0_R\}) \right\} \subseteq K$$

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 $\psi : \mathbf{Fr}(R) \longrightarrow K$ με $\iota = \psi \circ j$, όπου j ο μονομορφισμός (3.23). Για κάθε $(a, b) \in R \times (R \setminus \{0_R\})$ έχουμε

$$\psi(\tfrac{a}{b}) = \psi(j(a)j(b^{-1})) = \psi(j(ab^{-1})) = (\psi \circ j)(ab^{-1}) = \iota(ab^{-1}) = ab^{-1},$$

οπότε $\overline{R} = \mathrm{Im}(\psi) \cong \mathbf{Fr}(R)$. 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 $b \in R \setminus \{0_R\}$. Κατά συνέπειαν, το L περιέχει όλα τα στοιχεία τής μορφής ab^{-1}, όπου $(a, b) \in R \times (R \setminus \{0_R\})$. 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 $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, 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*

$$\mathbf{Fr}(f) : \mathbf{Fr}(R_1) \longrightarrow \mathbf{Fr}(R_2),\ \mathbf{Fr}(f)(\tfrac{a}{b}) := \tfrac{f(a)}{f(b)},\ \forall\, (a, b) \in R_1 \times (R_1 \setminus \{0_{R_1}\}),$$

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

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

ήτοι $\mathbf{Fr}(f)(\frac{a}{b}) = \frac{c}{d}$. Το (iii) είναι άμεση συνέπεια των (i) και (ii). □

3.6 ΠΡΩΤΑ ΣΩΜΑΤΑ

Έστω L ένα υπόσωμα τού σώματος $\mathbb{Q}$ των ρητών αριθμών. Επειδή υπάρχει πάντοτε κάποιο $a \in L \setminus \{0\}$, η -εξ ορισμού εγγυηθείσα- ύπαρξη τού (πολλαπλασιαστικού) αντιστρόφου του a^{-1} έχει ως επακόλουθο το ότι

$$a^{-1}a = 1_L = 1_{\mathbb{Q}} \in L.$$

Ως εκ τούτου, για κάθε ακέραιο $n \in \mathbb{Z}$ ισχύει $n = n \cdot 1_L = n \cdot 1_{\mathbb{Q}} \in L$, οπότε έχουμε κατ' ανάγκην την εγκλειστική σχέση $\mathbb{Z} \subseteq L \subseteq \mathbb{Q}$. Όμως, σύμφωνα με το πόρισμα 3.5.9, το $\mathbb{Q} = \mathbf{Fr}(\mathbb{Z})$ είναι το ελάχιστο σώμα (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την ακεραία περιοχή $\mathbb{Z}$. Άρα τελικώς $L = \mathbb{Q}$. Η ιδιότητα αυτή τού $\mathbb{Q}$ το καθιστά το πλέον τυπικό παράδειγμα των λεγομένων «πρώτων σωμάτων».

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

3.6.2 Παράδειγμα. Πέραν τού $\mathbb{Q}$, ένα άλλο πρώτο σώμα είναι το $\mathbb{Z}_p$, όπου p πρώτος αριθμός. Πράγματι· εάν το L είναι ένα υπόσωμα τού $\mathbb{Z}_p$, τότε η (προσθετική) υποομάδα $(L,+)$ τής ομάδας $(\mathbb{Z}_p,+)$ είναι πεπερασμένη με τάξη της έναν διαιρέτη τού p (λόγω τού θεωρήματος τού Lagrange). Επειδή λοιπόν ο p είναι πρώτος, $|L|=1$ ή $|L|=p$. Η πρώτη περίπτωση αποκλείεται, καθότι το L -ως σώμα- έχει τάξη $|L|\geq 2$. Επομένως, $|L|=p$, οπότε κατ' ανάγκην $L=\mathbb{Z}_p$.

3.6.3 Θεώρημα. *Κάθε σώμα K περιέχει ένα και μόνον πρώτο υπόσωμα.*

ΑΠΟΔΕΙΞΗ. Το σώμα

$$K_0 := \bigcap\{\, S \mid \ S \ \text{ υπόσωμα τού } K\} \subseteq K$$

είναι ένα πρώτο υπόσωμα τού K. Πράγματι· εάν το L είναι ένα υπόσωμα τού K_0, τότε το L είναι και υπόσωμα τού K, οπότε $K_0 \subseteq L$, απ' όπου συμπεραίνουμε ότι $L = K_0$. Υπολείπεται η απόδειξη τής μοναδικότητας τού K_0. Υποτιθεμένης τής 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 3.3.2,

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

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

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

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

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

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

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

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. □

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

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

3.6.6 Παρατήρηση. Σύμφωνα με όσα αναφέραμε στην απόδειξη τού θεωρήματος 3.6.4, εάν το L είναι ένα πρώτο σώμα, τότε

$$L \cong \left\{ (n \cdot 1_L)\,(m \cdot 1_L)^{-1} \;\middle|\; (n,m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\}, \quad \text{όταν } \chi\alpha\rho(L) = 0,$$

και

$$L = \;\{\, n \cdot 1_L \mid \; n \in \{0, 1, \ldots, p-1\}\}, \quad \text{όταν } \chi\alpha\rho(L) = p > 0.$$

Ασκήσεις

3-1. Ποιες εκ των ακολούθων απεικονίσεων $f : R \longrightarrow R'$ είναι ομομορφισμοί δακτυλίων;

(i) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k]_m .$$

(ii) $R = \mathbb{Z}$, $R' = \mathbb{Z}_m$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := [k+1]_m .$$

(iii) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a.$$

(iv) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := a + d.$$

(v) $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$, $R' = \mathbb{Z}$ και

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) := ad - bc.$$

(vi) $R = \mathbb{Z}$, $R' = \mathrm{Mat}_{2\times 2}(\mathbb{Z}_m)$ $(m \in \mathbb{N})$ και

$$k \longmapsto f(k) := \begin{pmatrix} [1]_m & [0]_m \\ [0]_m & [k]_m \end{pmatrix}.$$

3-2. (i) Να αποδειχθεί ότι η απεικόνιση

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5,\ n \longmapsto f(n) := ([n]_3 , [n]_5),$$

είναι επιμορφισμός και να προσδιορισθεί ο πυρήνας $\mathrm{Ker}(f)$.

(ii) Να προσδιορισθούν όλοι οι ομομορφισμοί $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_{12}$.

3-3. Να αποδειχθεί ότι οι μόνοι ενδομορφισμοί τού $\mathbb{Z}$ είναι ο μηδενικός ομομορφισμός και ο ταυτοτικός $\mathrm{id}_{\mathbb{Z}}$.

3-4. Έστω $m \in \mathbb{N}$. Να αποδειχθεί ότι κάθε ενδομορφισμός $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$ τού $\mathbb{Z}_m$ ορίζεται μέσω ενός τύπου τής μορφής

$$f([k]_m) = [a]_m [k]_m \,,\ \forall k \in \mathbb{Z},$$

για κάποιον ακέραιο a, τέτοιον ώστε το στοιχείο $[a]_m \in \mathbb{Z}_m$ να είναι ταυτοδύναμο.

3-5. Να αποδειχθεί ότι για κάθε ακέραιο m στερούμενον τετραγώνων η απεικόνιση

$$\mathbb{Q}(\sqrt{m}) \ni a + b\sqrt{m} \longmapsto a - b\sqrt{m} \in \mathbb{Q}(\sqrt{m}),\ \ a, b \in \mathbb{Z},$$

είναι αυτομορφισμός τού σώματος $\mathbb{Q}(\sqrt{m})$ (βλ. το (iv) τής ασκήσεως **1-37**).

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 $f(\text{Nil}(R)) \subseteq \text{Nil}(R')$).

Εν συνεχεία, να δοθούν παραδείγματα επιμορφισμών δακτυλίων για τους οποίους ο εγκλεισμός στο (i) είναι αυστηρός και τα αντίστροφα των (ii) και (iii) αναληθή.

3-11. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού R, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f(I + J) = f(I) + f(J)$,

(ii) $f(I\,J) = f(I)\; f(J)$,

(iii) $f(I \cap J) \subseteq f(I) \cap f(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$ ή $\text{Ker}(f) \subseteq J$).

(iv) Εάν ο R (και -κατ' επέκτασιν- και ο S, λόγω τής 3.1.9 (vii)) είναι μεταθετικός, τότε $f(I : J) \subseteq f(I) : f(J)$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$).

(v) Εάν ο R είναι μεταθετικός, τότε $f(\text{Rad}(I)) \subseteq \text{Rad}(f(I))$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν $\text{Ker}(f) \subseteq I$).

3-12. Έστω $f : R \longrightarrow S$ ένας επιμορφισμός δακτυλίων. Εάν τα I, J είναι ιδεώδη τού S, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(i) $f^{-1}(I + J) = f^{-1}(I) + f^{-1}(J)$,

(ii) $f^{-1}(I\,J) \supseteq f^{-1}(I)\; f^{-1}(J)$, (με τη σχέση αυτή ισχύουσα ως ισότητα

όταν $\mathrm{Ker}(f) \subseteq f^{-1}(I)\ f^{-1}(J)$),

(iii) $f^{-1}(I \cap J) = f^{-1}(I) \cap f^{-1}(J)$.

(iv) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(I : J) = f^{-1}(I) : f^{-1}(J)$.

(v) Εάν ο R είναι μεταθετικός, τότε $f^{-1}(\mathrm{Rad}(I)) = \mathrm{Rad}\big(f^{-1}(I)\big)$.

3-13. Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Υποτιθεμένου ότι $\chi\alpha\rho(R) > 0$, να αποδειχθεί ότι $\chi\alpha\rho(f(R)) \leq \chi\alpha\rho(R)$.

3-14. Να αποδειχθεί ότι ισόμορφοι δακτύλιοι έχουν ίσες χαρακτηριστικές.

3-15. Να αποδειχθεί ότι δεν υφίστανται μη μηδενικοί ομομορφισμοί δακτυλίων

$$f : R \longrightarrow R'$$

όταν ικανοποιείται μία εκ των κάτωθι συνθηκών:

(i) $\chi\alpha\rho(R) > 0 = \chi\alpha\rho(R')$.

(ii) $\chi\alpha\rho(R) > 0$, $\chi\alpha\rho(R') > 0$ και $\chi\alpha\rho(R') \nmid \chi\alpha\rho(R)$.

3-16. Εάν ο $f : K \longrightarrow L$ είναι ένας μονομορφισμός σωμάτων, να αποδειχθεί ότι $\chi\alpha\rho(K) = \chi\alpha\rho(L)$.

3-17. Έστω $f : R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων. Να αποδειχθούν τα εξής:

(i) Ο R' είναι ακεραία περιοχή εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι πρώτο ιδεώδες τού R.

(ii) Ο R' είναι σώμα εάν και μόνον εάν ο πυρήνας $\mathrm{Ker}(f)$ τού f είναι μεγιστικό ιδεώδες τού R.

3-18. Να αποδειχθεί ότι δεν υφίστανται ομομορφισμοί $f : \mathbb{C} \longrightarrow S$ (από το σώμα των μιγαδικών αριθμών σε έναν δακτύλιο S) με $\mathrm{Ker}(f) = \mathbb{Z}$.

3-19. Να αποδειχθεί ότι $\mathbb{Z}[\sqrt{3}] \ncong \mathbb{Z}[\sqrt{5}]$ και $\mathbb{Z}[\mathrm{X}] \ncong \mathbb{Q}[\mathrm{X}]$.

3-20. Έστω $f : R \longrightarrow S$ ένας ισομορφισμός δακτυλίων με μοναδιαία στοιχεία. Να αποδειχθούν τα ακόλουθα:

(i) Έστω $r \in R$. Τότε $r \in R^{\times} \Leftrightarrow f(r) \in S^{\times}$.

(ii) Η απεικόνιση $R^{\times} \ni r \longmapsto f(r) \in S^{\times}$ είναι αμφιριπτική.

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 3.3.2 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

$$f_E : \mathfrak{P}(M) \longrightarrow \mathfrak{P}(M), \quad A \longmapsto f_E(A) := A \cap (M \smallsetminus E)$$

είναι ομομορφισμός.

(iii) $\mathfrak{P}(M)/\mathfrak{P}(E) \cong \mathfrak{P}(M \smallsetminus E)$.

3-23. Έστω m ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθούν τα ακόλουθα:

(i) Το σύνολο

$$S := \left\{ \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

αποτελεί έναν υποδακτύλιο τού $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

(ii) Η απεικόνιση $f : \mathbb{Z}[\sqrt{m}] \longrightarrow S$ η οριζόμενη από τον τύπο

$$\mathbb{Z}[\sqrt{m}] \ni a + b\sqrt{m} \overset{f}{\longmapsto} \left(\begin{array}{cc} a & b \\ mb & a \end{array} \right) \in S$$

είναι ένας ισομορφισμός δακτυλίων. Ως εκ τούτου, ο S είναι μια ακεραία περιοχή. (Βλ. άσκηση **1-37** και το (i) τού πορίσματος 3.1.10.)

3-24. Να αποδειχθεί ότι $\mathbb{R}[\mathsf{X}]/\langle \mathsf{X}^2 \rangle \cong S$, όπου

$$S := \left\{ \left(\begin{array}{cc} a & b \\ 0 & a \end{array} \right) \;\middle|\; a, b \in \mathbb{R} \right\}.$$

[*Υπόδειξη*: Να δειχθεί ότι η απεικόνιση

$$\mathbb{R}[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i \longmapsto \left(\begin{array}{cc} a_0 & a_1 \\ 0 & a_0 \end{array} \right) \in S$$

είναι επιμορφισμός δακτυλίων έχων το κύριο ιδεώδες $\langle \mathsf{X}^2 \rangle$ ως πυρήνα του και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.2.]

3-25. Εάν $I := \langle \mathsf{X}^2 + 1 \rangle$ και $J := \langle \mathsf{X}^2 + 2 \rangle \subsetneqq \mathbb{R}[\mathsf{X}]$, 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 3.3.2 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 3.3.2.]

(iv) Ένα ιδεώδες I τού $\mathcal{C}([0,1])$ είναι μεγιστικό εάν και μόνον εάν $\exists \xi \in [0,1] : I = \mathfrak{m}_\xi$. [*Υπόδειξη*: Να γίνει κατάλληλη χρήση τής συμπάγειας τού κλειστού διαστήματος $[0,1]$.]

3-27. Έστω m ένας *θετικός* ακέραιος στερούμενος τετραγώνων και έστω

$$I_p(\sqrt{m}) := \left\{ a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \mid \text{με } \; p \mid a \text{ και } \; p \mid b \right\} \subsetneqq \mathbb{R},$$

όπου p περιττός πρώτος με $p \nmid m$. Να αποδειχθούν τα εξής:

(i) Το $I_p(\sqrt{m})$ είναι ένα ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$.

(ii) Εάν $n^2 \not\equiv m (\mathrm{mod}\, p)$, $\forall n \in \mathbb{Z}$, τότε το $I_p(\sqrt{m})$ είναι ένα μεγιστικό ιδεώδες τού $\mathbb{Z}[\sqrt{m}]$ και ο πηλικοδακτύλιος $\mathbb{Z}[\sqrt{m}]/I_p(\sqrt{m})$ ένα σώμα με p^2 στοιχεία.

3-28. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου R (όπου $n \in \mathbb{N},\ n \geq 2$), τότε το άθροισμά τους $I = I_1 + \cdots + I_n$ καλείται **(εσωτερικό) ευθύ άθροισμα**, σημειούμενο μέσω τού ειδικού συμβόλου $I_1 \oplus \cdots \oplus I_n$, όταν κάθε στοιχείο $a \in I$ εκφράζεται *μονοσημάντως* ως

$$a = a_1 + \cdots + a_n, \;\; a_j \in I_j, \;\; \forall j \in \{1, \ldots, n\}.$$

Να αποδειχθεί η ισοδυναμία των ακολούθων συνθηκών:

(i) Το I είναι το ευθύ άθροισμα των $I_1, \dots, I_n$.

(ii) Εάν $0_R = a_1 + \cdots + a_n$, όπου $a_j \in I_j,\ \forall j \in \{1, \dots, n\}$, τότε

$$a_1 = \cdots = a_n = 0_R.$$

(iii) $I_j \cap (\sum_{k \in \{1,\dots,n\} \setminus \{j\}} I_k) = \{0_R\},\ \forall j \in \{1, \dots, n\}$.

3-29. Να αποδειχθούν τα ακόλουθα:

(i) Εάν $R = R_1 \times \cdots \times R_n$ είναι το ευθύ γινόμενο n δακτυλίων $R_1, \dots, R_n$ (όπου $n \in \mathbb{N},\ n \geq 2$), και

$$\widetilde{R}_j := \left\{ \left(0_{R_1}, \dots, 0_{R_{j-1}}, a_j, 0_{R_{j+1}} \dots, 0_{R_n}\right) \in R \;\middle|\; a_j \in R_j \right\},$$

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 $I_1, \dots, I_n$ 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 $I_1, \dots, I_n$ θεωρούμενο ως «αυτόνομος» δακτύλιος (ήτοι ως το «εξωτερικό» ευθύ γινόμενο των $I_1, \dots, I_n$).

3-30. Έστω $R = R_1 \times \cdots \times R_n$ το ευθύ γινόμενο n δακτυλίων $R_1, \dots, R_n$ με μοναδιαία στοιχεία (όπου $n \in \mathbb{N},\ n \geq 2$). Να αποδειχθούν τα εξής:

(i) Για κάθε $j \in \{1, \dots, n\}$ η **προβολή** pr_j **τού** R **επί τού** R_j η οριζόμενη από τον τύπο

$$\mathrm{pr}_j : R \longrightarrow R_j,\ (a_1, \dots, a_n) \longmapsto \mathrm{pr}_j(a_1, \dots, a_n) := a_j,$$

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 $j \in \{1, \dots, n\}$. [*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 $j \in \{1, \dots, n\}$.

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

$$\boxed{R/I \cong (R/I_1) \oplus \cdots \oplus (R/I_n).}$$

[*Υπόδειξη*: Εάν ο $\varpi_j : R_j \longrightarrow R_j/I_j$ είναι ο φυσικός επιμορφισμός για κάθε $j \in \{1, \ldots, n\}$, να δειχθεί ότι η απεικόνιση

$$f : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n) \cong (R/I_1) \oplus \cdots \oplus (R/I_n)$$
$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n) := (\varpi_1(a_1), \ldots, \varpi_n(a_n))$$

είναι επιμορφισμός δακτυλίων με πυρήνα $\mathrm{Ker}(f) = I$ και να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών 3.3.2.]

3-33. (i) Εάν οι R και S είναι δυο δακτύλιοι και $I = \{(r, 0_S) \mid r \in R\}$, να αποδειχθεί ότι το I είναι ιδεώδες τού $R \times S$ και ότι

$$(R \times S)/I \cong S.$$

(ii) Εάν $m, n \in \mathbb{N}$, να αποδειχθεί ότι

$$(\mathbb{Z} \times \mathbb{Z}) / (m\mathbb{Z} \times n\mathbb{Z}) \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

3-34. Έστω R ένας μεταθετικός δακτύλιος ο οποίος περιέχει ένα ταυτοδύναμο στοιχείο c. Εάν

$$I := \{a \in R \mid ac = 0_R\}, \ \ J := \{a \in R \mid ac = a\},$$

να αποδειχθούν τα ακόλουθα:

(i) Τα I και J είναι ιδεώδη τού R.

(ii) $J = \langle c \rangle$.

(iii) $R \cong I \times J$.

(iv) $IJ = \{0_R\}$.

3-35. Έστω ότι ο R είναι ένας δακτύλιος, ο S ένας υποδακτύλιος τού R και το I ένα ιδεώδες τού R. Εάν $S \cap I = \{0_R\}$, να αποδειχθεί ότι ο S είναι ισόμορφος με έναν υποδακτύλιο τού πηλικοδακτυλίου R/I. [*Υπόδειξη*: Να χρησιμοποιηθεί το 2ο θεώρημα ισομορφισμών 3.3.14.]

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

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

τότε μέσω τής απεικονίσεως

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

τής επαγομένης από το $f(\mathsf{X})$ ορίζεται η απεικόνιση

$$R\,[\mathsf{X}] \longrightarrow \text{ΑΠ}\,(R, R) = R^R, \quad f(\mathsf{X}) \longmapsto \mathfrak{v}_{f(\mathsf{X})}.$$

καθώς και η **απεικόνιση πολυωνυμικής αποτιμήσεως σε ένα** (παγιωμένο) **στοιχείο** $r \in R$:

$$\varepsilon_r : R\,[\mathsf{X}] \longrightarrow R, \quad f(\mathsf{X}) \longmapsto \varepsilon_r(\, f(\mathsf{X})) := \mathfrak{v}_{f(\mathsf{X})}(r) := f(r)$$

(βλ. 1.3.11). Να αποδειχθούν τα ακόλουθα:

(i) Η $R\,[\mathsf{X}] \ni f(\mathsf{X}) \longmapsto \mathfrak{v}_{f(\mathsf{X})} \in R^R$ 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 $R\,[\mathsf{X}] \ni f(\mathsf{X}) \longmapsto \mathfrak{v}_{f(\mathsf{X})} \in R^R$ δεν είναι κατ' ανάγκην μονομορφισμός και, ως εκ τούτου, ο $R\,[\mathsf{X}]$ δεν είναι πάντοτε εμφυτεύσιμος στον R^R.]

(ii) Η ε_r είναι επιμορφισμός για κάθε $r \in R$.

3-38. Δοθέντος ενός ομομορφισμού $f : R \longrightarrow S$ μεταθετικών δακτυλίων με μοναδιαία στοιχεία και $f(1_R) = 1_S$, να αποδειχθεί ότι οι απεικονίσεις

$$\theta_f^{(1)} : R[\mathsf{X}] \longrightarrow S[\mathsf{X}], \qquad \theta_f^{(2)} : R[\![\mathsf{X}]\!] \longrightarrow S[\![\mathsf{X}]\!],$$
$$\theta_f^{(3)} : R[\mathsf{X}^{\pm 1}] \longrightarrow S[\mathsf{X}^{\pm 1}], \quad \theta_f^{(4)} : \text{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \longrightarrow \text{Laur}_S[\![\mathsf{X}^{\pm 1}]\!],$$

οι οριζόμενες μέσω των τύπων

$$R[\mathsf{X}] \ni \textstyle\sum_{i=0}^{n} a_i\mathsf{X}^i \overset{\theta_f^{(1)}}{\longmapsto} \sum_{i=0}^{n} f(a_i)\mathsf{X}^i \in S[\mathsf{X}],\ n \in \mathbb{N}_0,$$

$$R[\![\mathsf{X}]\!] \ni \textstyle\sum_{i=-n}^{\infty} a_i\mathsf{X}^i \overset{\theta_f^{(2)}}{\longmapsto} \sum_{i=-n}^{\infty} f(a_i)\mathsf{X}^i \in S[\![\mathsf{X}]\!],\ n \in \mathbb{N},$$

$$R[\mathsf{X}^{\pm 1}] \ni \textstyle\sum_{i=-n}^{m} a_i\mathsf{X}^i \overset{\theta_f^{(3)}}{\longmapsto} \sum_{i=-n}^{m} f(a_i)\mathsf{X}^i \in S[\mathsf{X}^{\pm 1}],\ m,n \in \mathbb{N},$$

$$\mathrm{Laur}_R[\![\mathsf{X}^{\pm 1}]\!] \ni \textstyle\sum_{i=-n}^{\infty} a_i\mathsf{X}^i \overset{\theta_f^{(4)}}{\longmapsto} \sum_{i=-n}^{\infty} f(a_i)\mathsf{X}^i \in \mathrm{Laur}_S[\![\mathsf{X}^{\pm 1}]\!],\ n \in \mathbb{N},$$

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

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

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*):

$$f(\mathsf{X}) \in R[\mathsf{X}]^\times \iff a_0 \in R^\times \ \text{ και } \ a_j \in \mathrm{Nil}(R),\ \forall j \in \{1,\dots,n\}.$$

[*Υπόδειξη*: Για την κατεύθυνση "$\Leftarrow$" να χρησιμοποιηθούν οι ασκήσεις **2**-**6** και **1**-**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 $\varpi : R \longrightarrow R/\mathfrak{p}$ και ο επαγόμενος επιμορφισμός

$$\theta_\varpi^{(1)} : R[\mathsf{X}] \longrightarrow (R/\mathfrak{p})[\mathsf{X}] \ \text{ με } \ \theta_\varpi^{(1)}(1_R) = 1_{R/\mathfrak{p}} = 1_R + \mathfrak{p}.$$

(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 3.1.9,

$$\sum_{i=0}^{n} \varpi(a_i)\mathsf{X}^i \in ((R/\mathfrak{p})[\mathsf{X}])^\times,$$

οπότε εφαρμόζοντας γι' αυτό το πολυώνυμο το πρώτο αποτέλεσμα τού (iii) τής προτάσεως 1.3.9 λαμβάνουμε

$$\varpi(a_0) \in ((R/\mathfrak{p})[\mathrm{X}])^{\times},\ \ \varpi(a_j) = 0_{R/\mathfrak{p}} = \mathfrak{p},\ \forall j \in \{1, \dots, n\}.$$

Από τις τελευταίες ισότητες έπεται ότι $a_j \in \mathfrak{p},\ \forall j \in \{1, \dots, n\}$. Επειδή το $\mathfrak{p}$ είναι αυθαιρέτως επιλεγμένο πρώτο ιδεώδες τού R, συμπεραίνουμε τελικώς ότι

$$a_j \in \bigcap \{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(R)\} = \mathrm{Nil}(R),\ \forall j \in \{1, \dots, n\},$$

κάνοντας χρήση τού (ii) τής ασκήσεως **2-37**.]

3-40. Να αποδειχθεί ότι για οιονδήποτε δακτύλιο R και οιονδήποτε $n \in \mathbb{N}$ η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R^{\mathrm{opp}}) \ni \mathbf{A} \longmapsto \mathbf{A}^t \in (\mathrm{Mat}_{n\times n}(R))^{\mathrm{opp}}$$

είναι ισομορφισμός, όπου R^{opp} είναι ο δακτύλιος ο αντικείμενος τού R (βλ. άσκηση **1-3**) και $\mathbf{A}^t$ 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

$$\boxed{\mathrm{Mat}_{n\times n}(R)[\mathrm{X}] \cong \mathrm{Mat}_{n\times n}(R[\mathrm{X}])} \quad \text{και} \quad \boxed{\mathrm{Mat}_{n\times n}(R)[\![\mathrm{X}]\!] \cong \mathrm{Mat}_{n\times n}(R[\![\mathrm{X}]\!]).}$$

3-42. Δοθέντος ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$ και ενός $n \in \mathbb{N}$ να αποδειχθεί ότι η απεικόνιση

$$\mathrm{Mat}_{n\times n}(R) \ni (a_{jk})_{1\le j,k\le n} \overset{\mathrm{Mat}_{n\times n}(f)}{\longmapsto} (f(a_{jk}))_{1\le j,k\le n} \in \mathrm{Mat}_{n\times n}(S),$$

είναι ομομορφισμός δακτυλίων και έχει τις εξής ιδιότητες:

(i) Η $\mathrm{Mat}_{n\times n}(f)$ είναι μονομορφισμός $\Leftrightarrow$ ο f είναι μονομορφισμός.

(ii) Η $\mathrm{Mat}_{n\times n}(f)$ είναι επιμορφισμός $\Leftrightarrow$ ο f είναι επιμορφισμός.

3-43. Έστω I ένα ιδεώδες ενός δακτυλίου R. Να αποδειχθεί ότι για κάθε $n \in \mathbb{N}$ υφίσταται κανονιστικός ισομορφισμός δακτυλίων

$$\boxed{\mathrm{Mat}_{n\times n}(R) \,/\, \mathrm{Mat}_{n\times n}(I) \cong \mathrm{Mat}_{n\times n}(R/I)}$$

[*Υπόδειξη*: Έστω $\varpi : R \longrightarrow R/I$ ο φυσικός επιμορφισμός. Να αποδειχθεί ότι ο επιμορφισμός

$$\mathrm{Mat}_{n\times n}(\varpi) : \mathrm{Mat}_{n\times n}(R) \longrightarrow \mathrm{Mat}_{n\times n}(R/I)$$

(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 3.3.2.]

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

$$\mathrm{Diag}_{n\times n}(R) := \{\, \mathrm{diag}(r_1, \ldots, r_n) \mid (r_1, \ldots, r_n) \in R^n \}$$

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 $\mathrm{SUT}_{n\times n}(R)$ είναι ένα ιδεώδες τού δακτυλίου $\mathrm{UT}_{n\times n}(R)$ και ο $\mathrm{LUT}_{n\times n}(R)$ ένα ιδεώδες τού δακτυλίου $\mathrm{LT}_{n\times n}(R)$. Να αποδειχθεί ότι

$$\mathrm{UT}_{n\times n}(R)/\mathrm{SUT}_{n\times n}(R) \cong \mathrm{Diag}_{n\times n}(R) \cong \mathrm{LT}_{n\times n}(R)/\mathrm{LUT}_{n\times n}(R).$$

3-45. Να προσδιορισθούν όλα τα ιδεώδη τού δακτυλίου $\mathrm{Mat}_{n\times n}(\mathbb{Z}_{12})$, όπου $n \in \mathbb{N}$. [*Υπόδειξη*: Να χρησιμοποιηθεί το εδάφιο 3.2.5 σε συνδυασμό με το το (vi) τής ασκήσεως **2-16**.]

3-46. Να προσδιορισθούν τα σύνολα λύσεων των συστημάτων γραμμικών ισοτιμιών:

$$\left\{ \begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{array} \right\}$$

και

$$\left\{ \begin{array}{l} 5x \equiv 6 \pmod 8 \\ 8x \equiv 10 \pmod{14} \\ 10x \equiv 5 \pmod{15} \end{array} \right\}$$

βάσει των τεχνικών που παρετέθησαν στην ενότητα 3.4.

3-47. Έστω m ένας ένας ακέραιος αριθμός στερούμενος τετραγώνων. Να αποδειχθεί ότι $\mathbf{Fr}(\mathbb{Z}[\sqrt{m}]) = \mathbb{Q}(\sqrt{m})$. [*Υπόδειξη*: Να γενικευθούν καταλλήλως τα προαναφερθέντα στο παράδειγμα 3.5.10.]

3-48. Έστω R μια ακεραία περιοχή. Να αποδειχθεί ότι $\mathrm{χαρ}(\mathbf{Fr}(R)) = \mathrm{χαρ}(R)$.

3-49. Να αποδειχθούν τα ακόλουθα:

(i) Έστω K ένα σώμα και έστω K_0 το (μοναδικό) πρώτο υπόσωμα τού K (βλ. θεώρημα 3.6.3). Εάν ο $f : K \longrightarrow K$ είναι ένας αυτομορφισμός τού K, τότε

$$f(a) = a,\ \forall a \in K_0.$$

Εξ αυτού έπεται, ειδικότερα, ότι η ταυτοτική απεικόνιση είναι ο μόνος αυτομορφισμός ενός πρώτου σώματος. [*Υπόδειξη*: Να χρησιμοποιηθεί η παρατήρηση 3.6.6.]

(ii) Δεν υπάρχουν άλλοι αυτομορφισμοί τού σώματος $\mathbb{R}$ των πραγματικών αριθμών πέραν τού ταυτοτικού. [*Υπόδειξη*: Είναι εύκολος ο έλεγχος τού ότι κάθε αυτομορφισμός $f : \mathbb{R} \longrightarrow \mathbb{R}$ τού $\mathbb{R}$ έχει την ιδιότητα: $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ (βάσει τού (i)) και διατηρεί τη συνήθη διάταξη τού $\mathbb{R}$. Να χρησιμοποιηθεί το γεγονός ότι κάθε πραγματικός αριθμός είναι το όριο μιας (συγκλίνουσας) ακολουθίας ρητών αριθμών.]

(iii) Το (ii) δεν είναι αληθές για το σώμα $\mathbb{C}$ και για το στρεβλό σώμα $\mathbb{H}_{\mathbb{R}}$. (Αρκεί η παράθεση ενός μη ταυτοτικού αυτομορφισμού για καθέναν εξ αυτών.)

3-50. Έστω R μια ακεραία περιοχή και έστω $\mathfrak{p} \in \mathrm{Spec}(R)$. Το

$$\boxed{R_{\mathfrak{p}} := \left\{ \tfrac{a}{b} \in \mathbf{Fr}(R) \middle|\, a \in R, b \in R \smallsetminus \mathfrak{p} \right\}}$$

καλείται **τοπικοποίηση τού** R **στο** $\mathfrak{p}$. Να αποδειχθούν τα εξής:

(i) Το $R_{\mathfrak{p}}$ είναι ένας υποδακτύλιος τού σώματος $\mathbf{Fr}(R)$ περιέχων τον R.

(ii) $\mathbf{Fr}(R) \cong \mathbf{Fr}(R_{\mathfrak{p}})$.

(iii) Ο $R_{\mathfrak{p}}$ είναι τοπικός δακτύλιος έχων το $\mathfrak{m}_{R_{\mathfrak{p}}} := \mathfrak{p}R_{\mathfrak{p}}$ ως το (μοναδικό) μεγιστικό του ιδεώδες.

(iv) $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \cong \mathbf{Fr}(R/\mathfrak{p})$.

(v) Όταν $R = \mathbb{Z}$ και $\mathfrak{p} = \langle p \rangle = p\mathbb{Z}$, όπου p κάποιος πρώτος αριθμός, ο $R_{\mathfrak{p}}$ είναι ο δακτύλιος των p-αδικών κλασμάτων $\mathbb{Z}_{\langle p \rangle}$ ο ορισθείς στην άσκηση **1-11** (σελ. 32) 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 $\mathbb{Z}_{\langle p \rangle}/p\mathbb{Z}_{\langle p \rangle} \cong \mathbb{Z}_p$.