

2. Δακτύλιοι

2.1 Βασικές έννοιες

2.2 Ακέραιες Περιοχές- Σώματα

2.3 Υποδακτύλιοι

2.4 Ιδεώδη

2.5 Χρήσιμα για συναρτήσεις

2.6 Ομομορφισμοί

2.7 Δακτύλιοι Πηλίκο - 1ο Θεώρημα Ισομορφισμού δακτυλίων

2.8 Κινέζικο Θεώρημα Υπολοίπων

2.9 Πρώτα - Μεγιστικά Ιδεώδη

2.10 Χαρακτηριστική Δακτυλίου

2.11 Λυμένα Προβλήματα

2.12 Άλυτα Προβλήματα

2. Δακτύλιοι

2.1 Βασικές έννοιες και παραδείγματα

Ορισμός 2.1.1.

Έστω A ένα μη κενό σύνολο. Μια απεικόνιση $*$: $A \times A \longrightarrow A$ θα καλείται **πράξη** επί του A . Για κάθε $(\alpha, \beta) \in A \times A$, την εικόνα της $*$ στο (α, β) θα τη θεωρούμε $\alpha * \beta$ αντί για $*((\alpha, \beta))$.

Παράδειγμα 2.1.2.

Η συνήθης πρόσθεση ακεραίων είναι μια διαδικασία που σε κάθε ζεύγος ακεραίων (m, n) αντιστοιχεί έναν νέο ακέραιο, τον οποίο θεωρούμε $m + n$ και ονομάζουμε άθροισμα των m, n .

Άρα η συνήθης πρόσθεση ακεραίων είναι μια απεικόνιση

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (m, n) \longmapsto m + n.$$

Ορισμός 2.1.3. Δακτυλίου

Έστω R ένα σύνολο εφοδιασμένο με δύο πράξεις

$$+ : R \times R \longrightarrow R, \quad (\alpha, \beta) \longmapsto \alpha + \beta$$

και

$$\cdot : R \times R \longrightarrow R, \quad (\alpha, \beta) \longmapsto \alpha \cdot \beta$$

τέτοιες ώστε να ισχύουν:

A. Για την πράξη $+$

(1) (Προσεταιριστική ιδιότητα) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, για κάθε $\alpha, \beta, \gamma \in R$.

(2) (Αντιμεταθετική ιδιότητα) $\alpha + \beta = \beta + \alpha$, για κάθε $\alpha, \beta \in R$.

(3) Υπάρχει ένα στοιχείο του R , το οποίο συμβολίζουμε με 0_R , ονομάζουμε μηδενικό στοιχείο του R και έχει την ιδιότητα $\alpha + 0_R = \alpha$, για κάθε $\alpha \in R$.

(4) Για κάθε $\alpha \in R$, υπάρχει ένα στοιχείο του R , το οποίο συμβολίζουμε με $-\alpha$, ονομάζουμε αντίθετο του α και έχει την ιδιότητα

$$\alpha + (-\alpha) = 0_R.$$

B. Για την πράξη $\cdot$ προσεταιριστική ιδιότητα, δηλαδή

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma), \quad \forall \alpha, \beta, \gamma \in R.$$

Γ. (Επιμεριστική ιδιότητα)

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \quad \text{και} \quad (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha,$$

για κάθε $\alpha, \beta, \gamma \in R$.

Τότε η τριάδα $(R, +, \cdot)$ καλείται **δακτύλιος**.

Η πράξη $+$ καλείται **πρόσθεση** του δακτυλίου R , ενώ η πράξη $\cdot$ καλείται **πολλαπλασιασμός** του δακτυλίου R .

Ορισμός 2.1.4.

Έστω $(R, +, \cdot)$ ένας δακτύλιος.

(1) Ο R θα καλείται **μεταθετικός δακτύλιος** εάν $\alpha\beta = \beta\alpha$, για κάθε $\alpha, \beta \in R$.

(2) Ο R θα καλείται **δακτύλιος με μοναδιαίο στοιχείο** εάν υπάρχει $\gamma \in R$ ώστε $\alpha\gamma = \alpha = \gamma\alpha$, για κάθε $\alpha \in R$.

Το γ συμβολίζεται με 1_R και καλείται **μοναδιαίο στοιχείο** του R .

Παραδείγματα 2.1.5

(i) Τα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, με τις συνήθεις πράξεις, είναι μεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο τον αριθμό 1.

(ii) Για κάθε $n \in \mathbb{N}$, ο $\mathbb{Z}_n$ είναι μεταθετικός δακτύλιος με μηδενικό στοιχείο την $[0]_n$, μοναδιαίο το $[1]_n$, με τις πράξεις $+$ και $\cdot$ που ορίστηκαν στο Κεφάλαιο 1, δηλαδή

$$[\alpha]_n + [\beta]_n = [\alpha + \beta]_n, \quad [\alpha]_n [\beta]_n = [\alpha\beta]_n.$$

(iii) Έστω $n \in \mathbb{N}$ και

$$M_n(\mathbb{R}) = \{\text{οι } n \times n \text{ πίνακες με στοιχεία πραγματικούς}\}.$$

Τότε ο $M_n(\mathbb{R})$, με τις συνήθεις πράξεις πινάκων, είναι δακτύλιος με μηδενικό στοιχείο τον μηδενικό πίνακα O_n και μοναδιαίο στοιχείο τον μοναδιαίο πίνακα I_n .

Για $n \geq 2$ ο $M_n(\mathbb{R})$ δεν είναι μεταθετικός.

(iv) Γενικότερα, εάν R δακτύλιος και

$$M_n(R) = \{\text{οι } n \times n \text{ πίνακες με στοιχεία από τον } R\},$$

αν ορίσουμε πρόσθεση και πολλαπλασιασμό στους $M_n(R)$ ανάλογα με τις πράξεις πινάκων με πραγματικούς αριθμούς, τότε ο $M_n(R)$ είναι δακτύλιος με μηδενικό στοιχείο τον πίνακα

$$O_n = \begin{pmatrix} 0_R & 0_R & \cdots & 0_R \\ 0_R & 0_R & \cdots & 0_R \\ \vdots & \vdots & \ddots & \vdots \\ 0_R & 0_R & \cdots & 0_R \end{pmatrix}.$$

Εάν ο R έχει μοναδιαίο στοιχείο, τότε και ο $M_n(R)$ έχει τον

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

(v) Παράδειγμα δακτυλίου χωρίς μοναδιαίο

Έστω $k \in \mathbb{Z}$ με $k \neq 0, 1, -1$. Θέτουμε

$$k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}.$$

Ο $k\mathbb{Z}$, με τις συνήθειες πράξεις ακεραίων, είναι μεταθετικός δακτύλιος με μηδενικό στοιχείο τον αριθμό 0.

Ο $k\mathbb{Z}$ δεν έχει μοναδιαίο.

Πράγματι, ας υποθέσουμε προς άτοπο ότι έχει το $1_{k\mathbb{Z}} = km$, όπου $m \in \mathbb{Z}$.

Επειδή $k \in k\mathbb{Z}$ και το $1_{k\mathbb{Z}} = km$ μοναδιαίο, έχουμε

$$k \cdot 1_{k\mathbb{Z}} = k \Rightarrow k \cdot km = k \Rightarrow km = 1$$

Τώρα αφού οι k, m είναι ακέραιοι και $km = 1$ έπεται ότι $k = m = 1$ ή $k = m = -1$. Άτοπο, αφού $k \neq 1, -1$.

Πρόταση 2.1.6.

Έστω $(R, +, \cdot)$ ένας δακτύλιος. Τότε

- (1) Το μηδενικό στοιχείο του R είναι μοναδικό.
- (2) Για κάθε $a \in R$, ο αντίθετος του a είναι μοναδικός και $-(-a) = a$.
- (3) $a \cdot 0_R = 0_R \cdot a = 0_R$, για κάθε $a \in R$.

- (4) $-0_R = 0_R$.
- (5) $-(a+b) = (-a) + (-b)$, για κάθε $a, b \in R$.
- (6) $(-a)b = a(-b) = -ab$ και $(-a)(-b) = ab$, για κάθε $a, b \in R$.
- (7) Αν $a, b, \delta \in R$ και $a + \delta = b + \delta$, τότε $a = b$.
- (8) Αν ο R έχει μοναδιαίο στοιχείο, τότε είναι μοναδικό.
- (9) Αν $a, b_1, \dots, b_n \in R$, τότε $a(b_1 + \dots + b_n) = ab_1 + \dots + ab_n$ και $(b_1 + \dots + b_n)a = b_1a + \dots + b_na$.

Απόδειξη.

- (1) Έστω ότι ο R έχει δύο μηδενικά στοιχεία, τα $0_R, 0'_R$. Τότε, αφού 0_R είναι μηδενικό στοιχείο, έχουμε $0'_R = 0_R + 0'_R$, ενώ αφού $0'_R$ είναι μηδενικό στοιχείο, έχουμε $0_R = 0_R + 0'_R$. Άρα $0_R = 0'_R$.
- (2) Έστω $a \in R$ και b, δ αντίθετοι του a . Τότε $b = b + 0_R = b + (a + \delta) = (b + a) + \delta = 0_R + \delta = \delta$. Επίσης, εφόσον ο αντίθετος είναι μοναδικός και $a + (-a) = (-a) + a = 0_R$, ο αντίθετος του $-a$ είναι ο a . Άρα $-(-a) = a$.
- (3) Έχουμε ότι $a \cdot 0_R = a(0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$. Άρα $a \cdot 0_R + [-(a \cdot 0_R)] = (a \cdot 0_R + a \cdot 0_R) + [-(a \cdot 0_R)]$, οπότε $0_R = a \cdot 0_R + (a \cdot 0_R + [-(a \cdot 0_R)]) = a \cdot 0_R + 0_R = a \cdot 0_R$. Άρα $a \cdot 0_R = 0_R$. Ομοίως $0_R \cdot a = 0_R$.
- (4) Άμεσο από το δεδομένο ότι $0_R + 0_R = 0_R$.
- (5) Για να δείξουμε ότι $-(a+b) = (-a) + (-b)$, αρκεί να δείξουμε ότι $a + b + ((-a) + (-b)) = 0_R$. Έχουμε
- $$\begin{aligned} a + b + ((-a) + (-b)) &= a + (b + ((-a) + (-b))) = a + (b + ((-b) + (-a))) \\ &= a + ((b + (-b)) + (-a)) = a + (0_R + (-a)) \\ &= a + (-a) = 0_R. \end{aligned}$$
- (6) Για να δείξουμε ότι $(-a)b = -ab$, αρκεί να δείξουμε ότι $(-a)b + ab = 0_R$. Έχουμε $(-a)b + ab = ((-a) + a)b = 0_R b = 0_R$. Ομοίως $a(-b) = -ab$. Επίσης, $(-a)(-b) = -a(-b) = -(-ab) = ab$.
- (7)–(9) Αφήνονται ως άσκηση.

Ορισμός 2.1.7.

Έστω $(R, +, \cdot)$ ένας δακτύλιος. Εάν $a, b \in R$, ορίζουμε τη **διαφορά** του a από το b να είναι η $a + (-b)$, συμβολικά $a - b$.

Εύκολα μπορούμε να δείξουμε ότι $a(b - \delta) = ab - a\delta$ και $(b - \delta)a = ba - \delta a$.

Ορισμός 2.1.8.

Έστω $(R, +, \cdot)$ ένας δακτύλιος και $a \in R$.

(1) Αν $n \in \mathbb{Z}$, ορίζουμε το n **φορές το** a και το συμβολίζουμε με na , να είναι το

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

(2) Εάν $n > 0$, ορίζουμε την n -**οστή δύναμη** του a να είναι το

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

Επίσης, εάν ο R έχει μοναδιαίο στοιχείο 1_R , ορίζουμε

$$a^0 = 1_R.$$

Πρόταση 2.1.9.

Έστω $(R, +, \cdot)$ δακτύλιος, $m, n \in \mathbb{Z}$ και $a, b \in R$. Τότε

(1) (i) $(m + n)a = ma + na$.

(ii) $n(a + b) = na + nb$.

(2) $n(ab) = (na)b = a(nb)$.

(3) $(ma)(nb) = (mn)(ab)$.

(4) $(-n)a = n(-a) = -(na)$.

(5) Εάν $m, n > 0$, τότε

$$(a^m)^n = a^{mn}, \quad a^m a^n = a^{m+n}.$$

(6) **Προσοχή!!** Δεν ισχύει πάντοτε ότι, αν $n \in \mathbb{Z}_{>0}$, τότε

$$(ab)^n = a^n b^n.$$

Αν όμως τα a, b αντιμετατίθενται, τότε

$$(ab)^n = a^n b^n.$$

Απόδειξη. Αφήνεται ως άσκηση.

Ορισμός 2.1.10.

Έστω R δακτύλιος με μοναδιαίο στοιχείο και $a \in R$.

Ένα $a \in R$ θα καλείται **αντιστρέψιμο**, εάν υπάρχει $b \in R$ ώστε

$$a \cdot b = b \cdot a = 1_R.$$

- Ο b καλείται **αντίστροφος** του a και συμβολίζεται με a^{-1} .
- Επίσης, θα συμβολίζουμε με $U(R)$ το σύνολο των αντιστρέψιμων στοιχείων του R , δηλαδή

$$U(R) = \{a \in R : a \text{ αντιστρέψιμο}\}.$$

Πρόταση 2.1.11.

Έστω R δακτύλιος με μοναδιαίο στοιχείο. Τότε

- (1) Αν $a \in U(R)$, ο αντίστροφος του a είναι μοναδικός.
- (2) Αν $a \in U(R)$, τότε $a^{-1} \in U(R)$ και $(a^{-1})^{-1} = a$.
- (3) $1_R, -1_R \in U(R)$.
- (4) Αν $a, b \in U(R)$, τότε $ab \in U(R)$ και $(ab)^{-1} = b^{-1}a^{-1}$.

Απόδειξη.

- (1) Έστω b, γ αντίστροφοι του a . Θα δείξουμε ότι $b = \gamma$.

Πράγματι,

$$b = b \cdot 1_R = b \cdot (a\gamma) = (ba)\gamma = 1_R\gamma = \gamma.$$

- (2) Εφόσον $aa^{-1} = a^{-1}a = 1_R$, έπεται ότι ο a^{-1} είναι αντιστρέψιμος με $(a^{-1})^{-1} = a$.

- (3) Παρατηρούμε ότι $1_R \cdot 1_R = 1_R$ και $(-1_R)(-1_R) = 1_R$. Άρα

$$1_R, -1_R \in U(R), \quad 1_R^{-1} = 1_R, \quad (-1_R)^{-1} = -1_R.$$

- (4) Έχουμε

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(1_Ra^{-1}) = aa^{-1} = 1_R,$$

και ομοίως $(b^{-1}a^{-1})(ab) = 1_R$. Άρα $ab \in U(R)$ και $(ab)^{-1} = b^{-1}a^{-1}$.

Παραδείγματα 2.1.12

(1) $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.

(2) $U(\mathbb{Z}) = \{-1, 1\}$.

(3) Αν $n \geq 2$, τότε, από την Πρόταση 1.7.14,

$$U(\mathbb{Z}_n) = \{[\alpha] : (\alpha, n) = 1\}.$$

(4) Έστω R μεταθετικός δακτύλιος με 1_R και

$$M_n(R) = \{\text{οι } n \times n \text{ πίνακες με στοιχεία από το } R\}.$$

Τότε

$$U(M_n(R)) = \{A \in M_n(R) : \det A \in U(R)\}.$$

Ειδικότερα,

$$U(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) : \det A \in \mathbb{R} \setminus \{0\}\},$$

ενώ

$$U(M_n(\mathbb{Z})) = \{A \in M_n(\mathbb{Z}) : \det A \in U(\mathbb{Z})\} = \{A \in M_n(\mathbb{Z}) : \det A = \pm 1\}.$$

(Η απόδειξη του (4) στηρίζεται στον προσαρτημένο πίνακα $\tilde{A}$ του A , για τον οποίο ισχύει $A\tilde{A} = \tilde{A}A = (\det A)I_n$, και στην $\det(AB) = \det A \det B$, και αφήνεται ως άσκηση.)

Παρατήρηση 2.1.13.

Σε όλους τους δακτυλίους τις πράξεις της πρόσθεσης και του πολλαπλασιασμού τις συμβολίζουμε με $+$ και $\cdot$, αντιστοίχως.

Τυπικά, εάν είχαμε δύο δακτυλίους R, S , ώστε οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στον R είναι διαφορετικές από αυτές του S , θα έπρεπε να τις συμβολίζουμε διαφορετικά. Για παράδειγμα, στον R με $+$, $\cdot$ και στον S με $\oplus, \odot$, ή, καλύτερα, στον R με $+_R, \cdot_R$ και στον S με $+_S, \cdot_S$.

Συνήθως δεν το κάνουμε αυτό, εκτός εάν είναι απαραίτητο (π.χ. εάν $R = S$). Θα πρέπει να έχουμε στο νου μας όμως ότι οι πράξεις στους R, S μπορεί να είναι διαφορετικές.

Για παράδειγμα, εάν $R = \mathbb{Z}$, $S = M_n(\mathbb{Z})$, άλλη είναι η διαδικασία της πρόσθεσης στο $\mathbb{Z}$ από αυτήν στο $M_n(\mathbb{Z})$.

Ένα παράδειγμα όπου $R = S$, αλλά οι πράξεις διαφέρουν.

Ας συμβολίσουμε με $+$, $\cdot$ τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού στο σύνολο των ακεραίων.

Έστω οι πράξεις $\oplus, \odot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ που ορίζονται ως εξής:

”Εάν $m, n \in \mathbb{Z}$, τότε $m \oplus n = m + n - 1$ και $m \odot n = mn - (m + n) + 2$.”

Με τις παραπάνω πράξεις το $\mathbb{Z}$ είναι δακτύλιος και μάλιστα

$$0_{\mathbb{Z}} = 1, \quad 1_{\mathbb{Z}} = 2.$$

(Γιατί;)

Ορισμός 2.1.14. Ευθύ γινόμενο δακτυλίων

Έστω R, S δύο δακτύλιοι. Στο καρτεσιανό γινόμενο $R \times S = \{(r, s) : r \in R, s \in S\}$ θεωρούμε τις πράξεις

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Με τις παραπάνω πράξεις ο $R \times S$ είναι δακτύλιος με μηδενικό στοιχείο το $0_{R \times S} = (0_R, 0_S)$ και ονομάζεται **ευθύ γινόμενο** των R, S .

Πρόταση 2.1.15.

Έστω R, S δύο δακτύλιοι και $R \times S$ το ευθύ γινόμενο αυτών. Τότε

- (1) Οι R, S μεταθετικοί αν και μόνο αν ο $R \times S$ μεταθετικός.
- (2) Οι R, S έχουν μοναδιαίο στοιχείο αν και μόνο αν ο $R \times S$ έχει μοναδιαίο.
- (3) Εάν οι R, S έχουν μοναδιαία, τότε $U(R \times S) = U(R) \times U(S)$.

Απόδειξη.

- (1) $(\Rightarrow)$ Έστω $(r_1, s_1), (r_2, s_2) \in R \times S$. Τότε

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_1) = (r_2, s_2) \cdot (r_1, s_1).$$

Άρα ο $R \times S$ είναι μεταθετικός.

$(\Leftarrow)$ Έστω $r_1, r_2 \in R, s_1, s_2 \in S$. Εφόσον ο $R \times S$ είναι μεταθετικός,

$$(r_1, s_1) \cdot (r_2, s_2) = (r_2, s_2) \cdot (r_1, s_1),$$

οπότε

$$(r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_1).$$

Άρα $r_1 r_2 = r_2 r_1$ και $s_1 s_2 = s_2 s_1$.

- (2) $(\Rightarrow)$ Έστω $1_R, 1_S$ τα μοναδιαία των R, S , αντιστοίχως. Παρατηρούμε ότι, για κάθε $(r, s) \in R \times S$,

$$(r, s) \cdot (1_R, 1_S) = (r \cdot 1_R, s \cdot 1_S) = (r, s)$$

και

$$(1_R, 1_S) \cdot (r, s) = (1_R \cdot r, 1_S \cdot s) = (r, s).$$

Άρα το $(1_R, 1_S)$ είναι μοναδιαίο του $R \times S$.

($\Leftarrow$) Έστω $1_{R \times S}$ το μοναδιαίο του $R \times S$ και έστω $1_{R \times S} = (r_0, s_0)$.

Έστω $r \in R, s \in S$. Τότε

$$(r, s) = (r, s) \cdot 1_{R \times S} = (r, s) \cdot (r_0, s_0) = (rr_0, ss_0)$$

και

$$(r, s) = 1_{R \times S} \cdot (r, s) = (r_0, s_0) \cdot (r, s) = (r_0r, s_0s).$$

Άρα $r = rr_0 = r_0r$ και $s = ss_0 = s_0s$. Επομένως το r_0 είναι μοναδιαίο του R και το s_0 μοναδιαίο του S .

(3) Θα δείξουμε πρώτα ότι $U(R) \times U(S) \subseteq U(R \times S)$.

Έστω $(r, s) \in U(R) \times U(S)$ με $r \in U(R), s \in U(S)$. Τότε

$$(r, s) \cdot (r^{-1}, s^{-1}) = (rr^{-1}, ss^{-1}) = (1_R, 1_S) = 1_{R \times S}$$

και

$$(r^{-1}, s^{-1}) \cdot (r, s) = (r^{-1}r, s^{-1}s) = (1_R, 1_S) = 1_{R \times S}.$$

Άρα το (r, s) είναι αντιστρέψιμο στον $R \times S$ και

$$(r, s)^{-1} = (r^{-1}, s^{-1}).$$

Ας αποδείξουμε τώρα ότι $U(R \times S) \subseteq U(R) \times U(S)$.

Έστω $(r, s) \in U(R \times S)$ και $(r_0, s_0) = (r, s)^{-1}$. Τότε

$$1_{R \times S} = (r, s) \cdot (r_0, s_0) \Rightarrow (1_R, 1_S) = (rr_0, ss_0) \Rightarrow rr_0 = 1_R, ss_0 = 1_S.$$

Ομοίως,

$$r_0r = 1_R, s_0s = 1_S.$$

Συνεπώς $r \in U(R), s \in U(S)$, άρα $(r, s) \in U(R) \times U(S)$.

Παράδειγμα 2.1.16.

Από το 2.1.15(3) έχουμε

$$U(\mathbb{Z}_6 \times \mathbb{Z}_{10}) = U(\mathbb{Z}_6) \times U(\mathbb{Z}_{10}).$$

Οπότε εφόσον

$$U(\mathbb{Z}_6) = \{[a]_6 : 1 \leq a \leq 5, (a, 6) = 1\} = \{[1]_6, [5]_6\}$$

και

$$U(\mathbb{Z}_{10}) = \{[a]_{10} : 1 \leq a \leq 9, (a, 10) = 1\} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}.$$

Άρα

$$U(\mathbb{Z}_6 \times \mathbb{Z}_{10}) = \{([1]_6, [1]_{10}), ([1]_6, [3]_{10}), ([1]_6, [7]_{10}), ([1]_6, [9]_{10}), ([5]_6, [1]_{10}), ([5]_6, [3]_{10}), ([5]_6, [7]_{10}), ([5]_6, [9]_{10})\}.$$

2.2 Ακέραιες περιοχές - Σώματα

Έστω $(R, +, \cdot)$ δακτύλιος. Τότε δεν ισχύει εν γένει ότι

$$ab = 0_R \Rightarrow a = 0_R \text{ ή } b = 0_R.$$

Για παράδειγμα,

(i) Στον $\mathbb{Z}_6$ έχουμε ότι $[2], [3] \neq [0]$, αλλά $[2][3] = [6] = [0]$.

(ii) Στον $M_2(\mathbb{R})$ έχουμε ότι, εάν $A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ -2 & -2 \end{pmatrix}$, τότε $AB = O$, αλλά $A \neq O$ και $B \neq O$.

Ορισμός 2.2.1.

Έστω $(R, +, \cdot)$ δακτύλιος και $a \in R$ με $a \neq 0_R$.

Θα λέμε ότι ο a είναι **αριστερός** (αντίστ. **δεξιός**) **μηδενοδιαιρέτης**, εάν υπάρχει $b \in R$ με $b \neq 0_R$, ώστε

$$ab = 0_R \quad (\text{αντίστ. } ba = 0_R).$$

Παρατηρούμε ότι

(i) Εάν ο a είναι αριστερός μηδενοδιαιρέτης και $b \in R$ ώστε $b \neq 0_R$ και $ab = 0_R$, τότε ο b είναι δεξιός μηδενοδιαιρέτης.

(ii) Εάν ο R είναι μεταθετικός δακτύλιος, τότε δεν υπάρχει διάκριση μεταξύ αριστερού και δεξιού μηδενοδιαιρέτη, οπότε λέμε απλώς ότι ο a είναι **μηδενοδιαιρέτης**.

Παραδείγματα 2.2.2

(α) Στον $\mathbb{Z}_6$ οι $[2], [3]$ είναι μηδενοδιαιρέτες, εφόσον $[2], [3] \neq [0]$ και $[2][3] = [0]$.

(β) Στον $M_2(\mathbb{R})$ ο $A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$ είναι αριστερός μηδενοδιαιρέτης και ο $B = \begin{pmatrix} 1 & 1 \\ -2 & -2 \end{pmatrix}$ δεξιός μηδενοδιαιρέτης, εφόσον $A, B \neq O$ και $AB = O$.

Πρόταση 2.2.3.

Έστω R δακτύλιος. Τα ακόλουθα είναι ισοδύναμα.

(1) Ο R δεν έχει μηδενοδιαιρέτες.

(2) Ισχύει ο πολλαπλασιαστικός νόμος της διαγραφής, δηλαδή εάν $a, b, \gamma \in R$ με $\gamma \neq 0_R$, τότε

$$a\gamma = b\gamma \Rightarrow a = b \quad \text{και} \quad \gamma a = \gamma b \Rightarrow a = b.$$

Απόδειξη.

(1) $\Rightarrow$ (2) Έστω $a, b, \gamma \in R$ με $\gamma \neq 0_R$ και $a\gamma = b\gamma$. Τότε

$$a\gamma = b\gamma \Rightarrow a\gamma - b\gamma = 0_R \Rightarrow (a - b)\gamma = 0_R.$$

Εάν $a - b \neq 0_R$, τότε, επειδή $\gamma \neq 0_R$, έχουμε ότι οι $a - b, \gamma$ είναι μηδενοδιαιρέτες. Άτοπο. Άρα $a - b = 0_R$, δηλαδή $a = b$.

Ομοίως, εάν $\gamma a = \gamma b$, τότε $\gamma(a - b) = 0_R$ και άρα $a = b$.

(2) $\Rightarrow$ (1) Έστω ότι ο R έχει μηδενοδιαιρέτες.

Τότε υπάρχουν $a, b \in R$ ώστε $a, b \neq 0_R$ και $ab = 0_R$.

Έχουμε

$$ab = 0_R = 0_R \cdot b.$$

Από την υπόθεση και επειδή $b \neq 0_R$, παίρνουμε $a = 0_R$, άτοπο.

Παρατηρήσεις 2.2.4

(α) Εάν R τετριμμένος δακτύλιος, δηλαδή $R = \{0_R\}$, τότε ο R έχει μοναδιαίο το $1_R = 0_R$.

(Πράγματι, εάν $r \in R$, τότε $r = 0_R$ και $r1_R = 0_R \cdot 0_R = 0_R = r$ και ομοίως $1_R r = r$.)

(β) Έστω R δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα

(i) Ο R δεν έχει μηδενοδιαιρέτες.

(ii) Εάν $a, b \in R$ με $ab = 0_R$, τότε $a = 0_R$ ή $b = 0_R$.

(Πράγματι, για το (i) $\Rightarrow$ (ii), έστω $a, b \in R$ με $ab = 0_R$. Εάν $a, b \neq 0_R$, τότε οι a, b είναι μηδενοδιαιρέτες. Άτοπο, εφόσον ο R δεν έχει μηδενοδιαιρέτες.

Για το (ii) $\Rightarrow$ (i), έστω ότι ο R έχει μηδενοδιαιρέτες. Τότε υπάρχουν $a, b \in R$ με $a, b \neq 0_R$ και $ab = 0_R$. Άτοπο, σύμφωνα με την υπόθεση.)

Ορισμός 2.2.5.

Ένας δακτύλιος R θα καλείται **ακέραια περιοχή** (α.π.) εάν

(1) ο R είναι μεταθετικός,

(2) ο R έχει μοναδιαίο στοιχείο $1_R \neq 0_R$,

- (3) ο R δεν έχει μηδενοδιαιρέτες ή, ισοδύναμα, ισχύει ότι εάν $a, b \in R$ με $ab = 0_R$, τότε $a = 0_R$ ή $b = 0_R$.

Παραδείγματα 2.2.6

- (1) Οι δακτύλιοι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, με τις συνήθεις πράξεις, είναι ακέραιες περιοχές.
(2) Για $n \geq 2$ ο $M_n(\mathbb{R})$ δεν είναι α.π. για δύο λόγους:

- (i) δεν είναι μεταθετικός,
(ii) δεν ισχύει ότι εάν $AB = O$, τότε $A = O$ ή $B = O$.

- (3) Ο $\mathbb{Z}_n$ είναι α.π. αν και μόνο αν ο n είναι πρώτος ($n \geq 2$).

Απόδειξη.

($\Leftarrow$) Γνωρίζουμε ότι ο $\mathbb{Z}_n$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο την $[1] \neq [0]$, αφού $n \geq 2$.

Έστω $[\alpha], [\beta] \in \mathbb{Z}_n$ με $[\alpha][\beta] = [0]$. Τότε

$$[\alpha][\beta] = [0] \Rightarrow [\alpha\beta] = [0] \Rightarrow n \mid \alpha\beta.$$

Εφόσον ο n είναι πρώτος,

$$n \mid \alpha \text{ ή } n \mid \beta \Rightarrow [\alpha] = [0] \text{ ή } [\beta] = [0].$$

Άρα ο $\mathbb{Z}_n$ είναι α.π.

($\Rightarrow$) Έστω ότι ο n δεν είναι πρώτος. Τότε υπάρχουν $\alpha, \beta \in \mathbb{Z}$ με $1 < \alpha < n$, $1 < \beta < n$, ώστε $n = \alpha\beta$.

Εφόσον $n = \alpha\beta$, έχουμε

$$[\alpha][\beta] = [\alpha\beta] = [n] = [0].$$

Επειδή ο $\mathbb{Z}_n$ είναι α.π.,

$$[\alpha] = [0] \text{ ή } [\beta] = [0] \Rightarrow n \mid \alpha \text{ ή } n \mid \beta,$$

άτοπο.

Άρα ο n είναι πρώτος.

- (4) Έστω R, S δύο δακτύλιοι με $R \neq \{0_R\}$, $S \neq \{0_S\}$. Τότε ο $R \times S$ έχει μηδενοδιαιρέτες και συνεπώς δεν είναι α.π.

(Πράγματι, έστω $r \in R$ με $r \neq 0_R$ και $s \in S$ με $s \neq 0_S$. Υπάρχουν αφού $R \neq \{0_R\}$, $S \neq \{0_S\}$. Θεωρούμε τα στοιχεία $(r, 0_S)$, $(0_R, s)$ του $R \times S$. Παρατηρούμε ότι

- (i) $(r, 0_S), (0_R, s) \neq (0_R, 0_S) = 0_{R \times S}$,
(ii) $(r, 0_S) \cdot (0_R, s) = (r \cdot 0_R, 0_S \cdot s) = (0_R, 0_S) = 0_{R \times S}$.

Άρα τα $(r, 0_S), (0_R, s)$ είναι μηδενοδιαϊρέτες του $R \times S$.)

(5) Ειδική περίπτωση του (4).

Ο $\mathbb{Q} \times \mathbb{Q}$ δεν είναι α.π. διότι έχει μηδενοδιαϊρέτες εφόσον για παράδειγμα $(1, 0), (0, 1) \neq (0, 0) = 0_{\mathbb{Q} \times \mathbb{Q}}$ και $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0_{\mathbb{Q} \times \mathbb{Q}}$.

Οπότε ο $\mathbb{Q} \times \mathbb{Q}$ όχι α.π., παρόλο που είναι μεταθετικός και έχει μοναδιαίο το $(1, 1) \neq (0, 0)$.

Ομοίως έχουμε ότι οι $\mathbb{Z} \times \mathbb{Z}, \mathbb{R} \times \mathbb{R}, \mathbb{Z}_n \times \mathbb{Z}_m$ ($n, m \geq 2$) δεν είναι α.π.

(6) Ο $\mathbb{Z}_3 \times \mathbb{Z}_1$ ή ο $\mathbb{Z} \times \mathbb{Z}_1$ είναι α.π.;

Ορισμός 2.2.7.

Ένας δακτύλιος R θα καλείται **σώμα** εάν

- (1) Ο R είναι μεταθετικός.
- (2) Ο R έχει μοναδιαίο στοιχείο $1_R \neq 0_R$.
- (3) Κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο. Δηλαδή $U(R) = R \setminus \{0_R\}$.
Συνήθως ένα σώμα το συμβολίζουμε με F ή K .

Παραδείγματα 2.2.8 (1) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα.

(2) Ο δακτύλιος $\mathbb{Z}$ δεν είναι σώμα, εφόσον $U(\mathbb{Z}) = \{-1, 1\}$.

(3) Εάν $n \in \mathbb{Z}_{>0}$ με $n \geq 2$, τότε

$$“\mathbb{Z}_n \text{ σώμα} \iff \text{o } n \text{ πρώτος.}”$$

Απόδειξη.

($\Leftarrow$) Γνωρίζουμε ότι ο $\mathbb{Z}_n$ είναι μεταθετικός με μοναδιαίο στοιχείο την $[1] \neq [0]$.

Επίσης, έστω $[\alpha] \in \mathbb{Z}_n$ με $[\alpha] \neq [0]$.

Εφόσον $[\alpha] \neq [0]$, έχουμε ότι $n \nmid \alpha$. Άρα, επειδή ο n είναι πρώτος, $(\alpha, n) = 1$.

Επομένως υπάρχουν $x, y \in \mathbb{Z}$ ώστε $xn + y\alpha = 1$. Άρα

$$[xn + y\alpha] = [1] \Rightarrow [xn] + [y][\alpha] = [1] \Rightarrow [0] + [y][\alpha] = [1] \Rightarrow [y][\alpha] = [1].$$

Επειδή ο $\mathbb{Z}_n$ είναι μεταθετικός, $[\alpha][y] = [1]$.

Άρα το $[\alpha]$ είναι αντιστρέψιμο.

($\Rightarrow$) Θα δείξουμε ότι $(\alpha, n) = 1$ για κάθε $\alpha \in \{1, \dots, n-1\}$.

Πράγματι, έστω $\alpha \in \{1, \dots, n-1\}$. Τότε $[\alpha] \neq [0]$ και, επειδή ο $\mathbb{Z}_n$ είναι σώμα, το $[\alpha]$ είναι αντιστρέψιμο.

Άρα υπάρχει $\beta \in \{1, \dots, n-1\}$ ώστε $[\alpha][\beta] = [1]$.

Επομένως

$$[\alpha\beta] = [1] \Rightarrow \alpha\beta \equiv 1 \pmod{n} \Rightarrow n \mid (\alpha\beta - 1).$$

Άρα υπάρχει $k \in \mathbb{Z}$ ώστε $\alpha\beta - 1 = kn$, δηλαδή $\alpha\beta - kn = 1$. Επομένως $(\alpha, n) = 1$.

Άρα ο n δεν έχει θετικό διαιρέτη d με $1 < d < n$, δηλαδή ο n είναι πρώτος.

Πρόταση 2.2.9.

(1) Κάθε σώμα είναι ακέραια περιοχή.

(2) Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη.

(1) Έστω F σώμα. Δεδομένου ότι το F είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1_F \neq 0_F$, για να δείξουμε ότι το F είναι α.π., αρκεί να αποδείξουμε ότι

$$\text{“εάν } a, b \in F \text{ με } ab = 0_F, \text{ τότε } a = 0_F \text{ ή } b = 0_F\text{”}.$$

Έστω λοιπόν $a, b \in F$ με $ab = 0_F$.

Έστω ότι $a \neq 0_F$. Εφόσον το F είναι σώμα, υπάρχει ο a^{-1} .

Συνεπώς

$$ab = 0_F \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0_F \Rightarrow (a^{-1}a)b = 0_F \Rightarrow 1_F \cdot b = 0_F \Rightarrow b = 0_F.$$

Ομοίως, εάν $b \neq 0_F$, τότε $a = 0_F$.

Άρα $a = 0_F$ ή $b = 0_F$.

(2) Έστω R α.π. με πεπερασμένο πλήθος στοιχείων.

Εφόσον ο R είναι α.π., έχουμε ότι είναι μεταθετικός με μοναδιαίο $1_R \neq 0_R$.

Οπότε, για να δείξουμε ότι ο R είναι σώμα, αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο.

Έστω ότι τα στοιχεία του R είναι τα

$$a_0 = 0_R, \quad a_1 = 1_R, \quad a_2, \dots, a_n,$$

δηλαδή

$$R = \{0_R = a_0, 1_R = a_1, a_2, \dots, a_n\},$$

με $a_i \neq a_j$ για κάθε $i \neq j$.

Έστω $a \in R$ με $a \neq 0_R$. Για να δείξουμε ότι ο a είναι αντιστρέψιμος, αρκεί να δείξουμε ότι υπάρχει $i \in \{1, \dots, n\}$ ώστε $aa_i = 1_R$.

Θέτουμε

$$B = \{aa_1, aa_2, \dots, aa_n\} \subseteq R.$$

Παρατηρούμε ότι:

(i) $aa_i \neq 0_R$ για κάθε $i = 1, \dots, n$.

Πράγματι, εάν $aa_i = 0_R$, τότε, επειδή ο R είναι α.π. και $a \neq 0_R$, θα είχαμε $a_i = 0_R$, άτοπο.

(ii) $aa_i \neq aa_j$ για κάθε $i, j \in \{1, \dots, n\}$ με $i \neq j$.

Πράγματι, εάν $aa_i = aa_j$, τότε, από τον νόμο διαγραφής στην α.π. (Πρόταση 2.2.3), επειδή $a \neq 0_R$, παίρνουμε $a_i = a_j$, άτοπο.

Επομένως όλα τα στοιχεία του B είναι μη μηδενικά και τα μη μηδενικά στοιχεία του R είναι τα $\{a_1, a_2, \dots, a_n\}$. Άρα

$$B \subseteq \{a_1, a_2, \dots, a_n\}. \quad (1)$$

Επίσης, από το (ii), τα στοιχεία του B είναι ανά δύο διαφορετικά. Επομένως το B έχει ακριβώς n στοιχεία. Από την (1) συμπεραίνουμε ότι

$$B = \{a_1, a_2, \dots, a_n\} = \{1_R, a_2, \dots, a_n\}.$$

Άρα υπάρχει $i \in \{1, \dots, n\}$ ώστε $aa_i = 1_R$.

Επομένως ο a είναι αντιστρέψιμος και συνεπώς ο R είναι σώμα.

Παρατήρηση 2.2.10.

Το αντίστροφο του (1) δεν ισχύει γενικά.

Για παράδειγμα, ο $\mathbb{Z}$ είναι ακέραια περιοχή αλλά όχι σώμα.

2.3 Υποδακτύλιοι

Ορισμός 2.3.1.

Έστω A ένα σύνολο εφοδιασμένο με μία πράξη $*$. Έστω $B \subseteq A$. Θα λέμε ότι το B είναι **κλειστό ως προς την $*$** , εάν $b_1 * b_2 \in B$ για κάθε $b_1, b_2 \in B$.

Παραδείγματα 2.3.2

Έστω $A = \mathbb{R}$, $* = +$.

(i) Το $\mathbb{Q}$ είναι κλειστό ως προς την $+$.

(ii) Το $\mathbb{R} \setminus \mathbb{Q}$ δεν είναι κλειστό ως προς την $+$.

Ορισμός 2.3.3.

Έστω $(R, +, \cdot)$ ένας δακτύλιος και $S \subseteq R$.

Το S θα καλείται **υποδακτύλιος** του R , εάν

(i) $S \neq \emptyset$.

(ii) Το S είναι κλειστό ως προς τις πράξεις $+$, $\cdot$ του R .

(iii) Το S , με τις πράξεις $+$, $\cdot$, είναι δακτύλιος.

(Για την ακρίβεια, το S με τις $+\mid_{S \times S}$, $\cdot\mid_{S \times S}$ είναι δακτύλιος.)

Πρόταση 2.3.4.

Έστω S υποδακτύλιος του R και $0_S, 0_R$ τα μηδενικά των S, R , αντιστοίχως. Τότε $0_R \in S$ και $0_S = 0_R$.

Απόδειξη.

Έστω $s \in S$ (υπάρχει αφού το $S \neq \emptyset$).

Στον δακτύλιο S ισχύει $s + 0_S = s$, ενώ στον δακτύλιο R ισχύει $s + 0_R = s$. Άρα $s + 0_S = s + 0_R$ και, από τον νόμο διαγραφής στον R , παίρνουμε $0_S = 0_R$.

Εφόσον $0_S \in S$, έπεται ότι και $0_R \in S$.

Πρόταση 2.3.5.

Έστω R δακτύλιος και $S \subseteq R$ μη κενό. Τ.Α.Ε.Ι.

(1) Το S είναι υποδακτύλιος του R .

(2) $s_1 + s_2, s_1 s_2, -s \in S$, για κάθε $s_1, s_2, s \in S$.

Απόδειξη. Αφήνεται ως άσκηση.

Παραδείγματα 2.3.6

(1) Ο $\mathbb{Z}$ υποδακτύλιος του $\mathbb{Q}$.

Ο $\mathbb{Q}$ υποδακτύλιος του $\mathbb{R}$.

Το $\mathbb{R}$ υποδακτύλιος του $\mathbb{C}$.

Ο $k\mathbb{Z}$ υποδακτύλιος του $\mathbb{Z}$.

Ο $\mathbb{R} \setminus \mathbb{Q}$ δεν είναι υποδακτύλιος του $\mathbb{R}$.

(2) (Επεκτάσεις του $\mathbb{Q}$)

Έστω p πρώτος. Θέτουμε $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$. Τότε

(i) $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{R}$.

(ii) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p})$ (αφού αν $a \in \mathbb{Q}$, τότε $a = a + 0\sqrt{p}$).

(iii) $\mathbb{Q} \neq \mathbb{Q}(\sqrt{p})$ (αφού $\sqrt{p} = 0 + 1\sqrt{p} \in \mathbb{Q}(\sqrt{p})$, αλλά $\sqrt{p} \notin \mathbb{Q}$). Άρα, από τα (ii),
(iii), $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{p})$.

(iv) Ο $\mathbb{Q}(\sqrt{p})$ είναι υποδακτύλιος του $\mathbb{R}$ και μάλιστα σώμα (για $p = 2$ βλ. 11ο λυμένο, ενώ η γενική περίπτωση είναι ανάλογη).

(3) (Επεκτάσεις του $\mathbb{Z}$)

Αναλόγως με πριν, εάν p πρώτος,

$$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}.$$

Ισχύουν

$$\mathbb{Z}[\sqrt{p}] \subseteq \mathbb{R}, \quad \mathbb{Z} \subsetneq \mathbb{Z}[\sqrt{p}],$$

και ο $\mathbb{Z}[\sqrt{p}]$ είναι υποδακτύλιος του $\mathbb{R}$ αλλά και του $\mathbb{Q}(\sqrt{p})$.

Παρατηρήσεις 2.3.7 Μοναδιαίο στοιχείο και υποδακτύλιος

- (1) Αν ο R έχει μοναδιαίο στοιχείο, αυτό δεν σημαίνει ότι και ο S έχει μοναδιαίο στοιχείο.

Για παράδειγμα, ο $2\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Z}$ και δεν έχει μοναδιαίο στοιχείο, παρόλο που ο $\mathbb{Z}$ έχει μοναδιαίο στοιχείο.

- (2) Μπορεί και ο R και ο S να έχουν μοναδιαίο στοιχείο και να μην είναι ίσα.

Για παράδειγμα, εάν $R = \mathbb{Z}_6$ και $S = \{[0], [2], [4]\}$, εύκολα παρατηρούμε ότι ο S είναι υποδακτύλιος του R . Επίσης, η $[4]$ είναι μοναδιαίο του S , διότι

$$[0][4] = [0] = [4][0], \quad [2][4] = [2] = [4][2], \quad [4][4] = [4] = [4][4].$$

Συνεπώς $1_R = [1] \neq [4] = 1_S$.

- (3) Αν ο R έχει μοναδιαίο στοιχείο 1_R και αυτό ανήκει στον S , τότε το 1_R είναι μοναδιαίο και του S .

Πράγματι, εάν $s \in S$, τότε $s1_R = s = 1_R s$.

- (4) Αν ο R είναι α.π., $S \neq \{0_R\}$ και ο S έχει μοναδιαίο στοιχείο το 1_S , τότε $1_S = 1_R$.

Πράγματι, εάν $s \in S$ με $s \neq 0_R$, τότε

$$s = s1_S, \quad s = s1_R.$$

Άρα $s1_S = s1_R$, οπότε $s(1_S - 1_R) = 0_R$. Επειδή ο R είναι α.π. και $s \neq 0_R$, έπεται ότι $1_S - 1_R = 0_R$, δηλαδή $1_S = 1_R$.

Παρατηρήσεις 2.3.8

- (1) Εάν F σώμα και S υποδακτύλιος του F , τότε το S δεν είναι πάντοτε σώμα.

Για παράδειγμα, $F = \mathbb{R}$, $S = \mathbb{Z}$.

- (2) Εάν ο R δακτύλιος όχι σώμα και S υποδακτύλιος του R , τότε, όπως φαίνεται στα λυμένα 13 και 19, ο S μπορεί και να είναι σώμα.

Πρόταση 2.3.9.

Έστω R δακτύλιος και $\{S_i\}_{i \in I}$ μία οικογένεια υποδακτυλίων του R . Τότε η $\bigcap_{i \in I} S_i$ είναι υποδακτύλιος του R .

Απόδειξη.

Εφόσον κάθε S_i είναι υποδακτύλιος του R , έχουμε $0_R \in S_i$ για κάθε $i \in I$. Άρα $0_R \in \bigcap_{i \in I} S_i$, οπότε $\bigcap_{i \in I} S_i \neq \emptyset$. Έστω τώρα $s_1, s_2, s \in \bigcap_{i \in I} S_i$. Τότε, για κάθε $i \in I$, έχουμε $s_1, s_2, s \in S_i$. Επειδή κάθε S_i είναι υποδακτύλιος του R , παίρνουμε $s_1 + s_2, s_1 s_2, -s \in S_i$, για κάθε $i \in I$.

Επομένως $s_1 + s_2, s_1 s_2, -s \in \bigcap_{i \in I} S_i$. Άρα, από την Πρόταση 2.3.5, η $\bigcap_{i \in I} S_i$ είναι υποδακτύλιος του R .

Παρατήρηση 2.3.10.

Είδαμε στην Πρόταση 2.3.9 ότι η τομή υποδακτυλίων είναι υποδακτύλιος. Δεν ισχύει εν γένει το ίδιο για την ένωση.

Για παράδειγμα, έστω $R = \mathbb{Z}$, $S = 3\mathbb{Z}$, $T = 2\mathbb{Z}$.

Οι S, T είναι υποδακτύλιοι του $\mathbb{Z}$.

Εάν το $S \cup T$ ήταν υποδακτύλιος του $\mathbb{Z}$, τότε, επειδή $3, 2 \in S \cup T$, θα έπρεπε να ισχύει και

$$3 + 2 = 5 \in S \cup T.$$

Όμως $5 \notin 3\mathbb{Z}$ και $5 \notin 2\mathbb{Z}$, άρα $5 \notin S \cup T$, άτοπο.

Επομένως το $S \cup T$ δεν είναι υποδακτύλιος του $\mathbb{Z}$.

2.4 Ιδεώδη

Ορισμός 2.4.1.

Έστω R δακτύλιος και $I \subseteq R$. Το I θα καλείται **ιδεώδες** του R , εάν

- (1) Είναι μη κενό
- (2) $a - b \in I$, για κάθε $a, b \in I$.
- (3) $ra, ar \in I$, για κάθε $a \in I, r \in R$.

Παρατηρήσεις 2.4.2

(α) Αν ο R είναι μεταθετικός δακτύλιος, τότε η (3) του ορισμού μπορεί να αντικατασταθεί με την

$$(3)' \quad ar \in I, \text{ για κάθε } a \in I, r \in R.$$

(β) Αν I ιδεώδες του R , τότε το I είναι υποδακτύλιος.

Απόδειξη.

Αρκεί, σύμφωνα με την Πρόταση 2.3.5, να δείξουμε ότι

(i) $s_1 + s_2, s_1 s_2 \in I$, για κάθε $s_1, s_2 \in I$.

(ii) $-s \in I$, για κάθε $s \in I$.

Έστω $\delta \in I$ (υπάρχει εφόσον $I \neq \emptyset$). Επειδή το I είναι ιδεώδες, $\delta - \delta = 0_R \in I$.

Έστω τώρα $s \in I$. Επειδή $0_R, s \in I$, έχουμε $0_R - s = -s \in I$. Άρα ισχύει η (ii).

Έστω τώρα $s_1, s_2 \in I$. Επειδή το I είναι ιδεώδες, για $r = s_1 \in R$ και $a = s_2 \in I$, έχουμε $s_1 s_2 = ra \in I$.

Επίσης, αφού $-s_2 \in I$, παίρνουμε $s_1 - (-s_2) = s_1 + s_2 \in I$.

Άρα ισχύει και η (i).

(γ) Το αντίστροφο του (β) εν γένει δεν ισχύει.

Για παράδειγμα, ο $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Q}$, αλλά όχι ιδεώδες. Πράγματι, εάν ήταν, τότε, επειδή $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, θα είχαμε $1 \cdot \frac{1}{2} = \frac{1}{2} \in \mathbb{Z}$, άτοπο.

(δ) Αν ο R είναι δακτύλιος με μοναδιαίο στοιχείο 1_R και I ιδεώδες του R με $1_R \in I$, τότε $I = R$.

Πράγματι, εάν $r \in R$, τότε, επειδή I είναι ιδεώδες και $1_R \in I$, έχουμε $r1_R \in I$.

Άρα $r \in I$, οπότε $R \subseteq I$. Εφόσον πάντοτε $I \subseteq R$, έπεται ότι $I = R$.

Παραδείγματα 2.4.3

(α) Εάν R δακτύλιος, τότε τα $\{0_R\}$, R είναι ιδεώδη του R και καλούνται τετριμμένα ιδεώδη του R .

(β) Για κάθε $n \in \mathbb{Z}$, το σύνολο των πολλαπλασίων του n

$$n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$$

είναι ιδεώδες του $\mathbb{Z}$.

(γ) (Κύρια ιδεώδη)

Έστω R μεταθετικός δακτύλιος και $a \in R$. Το

$$I = \{ra : r \in R\}$$

είναι ιδεώδες του R , το συμβολίζουμε με $\langle a \rangle$ και καλείται το **κύριο ιδεώδες** του R που παράγεται από το a .

Έχουμε λοιπόν

$$\langle a \rangle = \{ra : r \in R\}.$$

Για παράδειγμα, στον $\mathbb{Z}$,

$$\langle n \rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z},$$

ενώ στον $\mathbb{Z}_8$,

$$\begin{aligned}\langle [2] \rangle &= \{[\alpha] \cdot [2] : \alpha \in \{0, 1, \dots, 7\}\} \\ &= \{[0], [2], [4], [6], [8], [10], [12], [14]\} \\ &= \{[0], [2], [4], [6]\},\end{aligned}$$

αφού $[8] = [0]$, $[10] = [2]$, $[12] = [4]$, $[14] = [6]$.

(δ) (Γενίκευση του (γ))

Έστω R μεταθετικός δακτύλιος και $a_1, a_2, \dots, a_n \in R$. Τότε το

$$I = \{r_1 a_1 + \dots + r_n a_n : r_1, \dots, r_n \in R\}$$

είναι ιδεώδες του R και συμβολίζεται με

$$I = \langle a_1, a_2, \dots, a_n \rangle.$$

Για παράδειγμα, έστω $R = \mathbb{Z}$, $I = \langle 4, 10 \rangle$. Τότε

$$I = \{4m + 10k : m, k \in \mathbb{Z}\}.$$

Παρατηρήσεις 2.4.4

Έστω R μεταθετικός δακτύλιος, $a \in R$ και το κύριο ιδεώδες $\langle a \rangle$ που παράγεται από το a . Τότε

(1) Εάν ο R έχει μοναδιαίο στοιχείο, τότε $a \in \langle a \rangle$.

Πράγματι, εφόσον $\langle a \rangle = \{ra : r \in R\}$, για $r = 1_R$ έχουμε $a = 1_R a \in \langle a \rangle$.

(2) Εν γένει δεν ισχύει $a \in \langle a \rangle$.

Για παράδειγμα, εάν $R = 2\mathbb{Z}$, $a = 4 \in R$, τότε

$$\langle 4 \rangle = \{r4 : r \in 2\mathbb{Z}\} = \{(2k)4 : k \in \mathbb{Z}\} = \{8k : k \in \mathbb{Z}\},$$

δηλαδή το σύνολο των πολλαπλασίων του 8.

Είναι σαφές ότι $4 \notin \langle 4 \rangle$.

Επομένως, όταν ο R δεν έχει μοναδιαίο στοιχείο, το $\langle a \rangle$ δεν είναι εν γένει το μικρότερο ιδεώδες του R που περιέχει το a , και η έκφραση “παράγεται από το a ” είναι ακριβής όταν ο R έχει μοναδιαίο στοιχείο.

Θεώρημα 2.4.5.

Εάν S υποδακτύλιος του $\mathbb{Z}$ τότε υπάρχει $d \in \mathbb{Z}$, $d \geq 0$, ώστε $S = \langle d \rangle = d\mathbb{Z}$.

Άρα κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο ιδεώδες.

Απόδειξη.

Θα δείξουμε ότι, εάν S είναι υποδακτύλιος του $\mathbb{Z}$, τότε υπάρχει $d \geq 0$ ώστε $S = d\mathbb{Z} = \langle d \rangle$. Από αυτό έπεται ότι κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο, αφού κάθε ιδεώδες είναι υποδακτύλιος.

Έστω λοιπόν S υποδακτύλιος του $\mathbb{Z}$.

Εάν $S = \{0\}$, τότε $S = 0\mathbb{Z}$.

Έστω τώρα $S \neq \{0\}$ και

$d = \text{το ελάχιστο θετικό στοιχείο του } S.$

(Κοίτα στο τέλος της απόδειξης γιατί υπάρχει το d)

Θα δείξουμε ότι $S = d\mathbb{Z}$. Καταρχάς $d\mathbb{Z} \subseteq S$.

Πράγματι, έστω $n \in \mathbb{Z}$.

Εάν $n > 0$, τότε $dn = \underbrace{d + \cdots + d}_{n \text{ φορές}} \in S$, αφού $d \in S$ και το S είναι υποδακτύλιος.

Εάν $n < 0$, τότε $dn = \underbrace{(-d) + \cdots + (-d)}_{-n \text{ φορές}} \in S$, αφού $-d \in S$.

Τέλος, για $n = 0$ έχουμε $dn = 0 \in S$. Άρα $d\mathbb{Z} \subseteq S$.

Ας δείξουμε τώρα ότι $S \subseteq d\mathbb{Z}$.

Έστω $m \in S$. Από την ταυτότητα της διαίρεσης υπάρχουν $q, r \in \mathbb{Z}$ με $m = dq + r$ όπου $0 \leq r < d$.

Τότε $r = m - dq$. Εφόσον $m, dq \in S$, έχουμε $r \in S$.

Αν ήταν $r > 0$, τότε θα είχαμε $0 < r < d$, άτοπο από την επιλογή του d ως ελάχιστου θετικού στοιχείου του S . Άρα $r = 0$ και συνεπώς $m = dq \in d\mathbb{Z}$. Άρα $S \subseteq d\mathbb{Z}$.

Μένει να δείξουμε ότι υπάρχει το d . Θέτουμε $A = \{m \in S : m > 0\}$. Το A είναι μη κενό. Πράγματι, έστω $s \in S$ με $s \neq 0$.

Αν $s > 0$, τότε $s \in A$.

Αν $s < 0$, τότε $-s > 0$ και, επειδή S είναι υποδακτύλιος, $-s \in S$, άρα $-s \in A$.

Εφόσον το A είναι μη κενό υποσύνολο των φυσικών, διαθέτει ελάχιστο στοιχείο, το οποίο είναι το d .

Ορισμός 2.4.6. Άθροισμα και γινόμενο ιδεωδών

Έστω R δακτύλιος και I, J ιδεώδη του R .

Ορίζουμε

(1) Το άθροισμα των I, J να είναι το

$$I + J = \{a + b : a \in I, b \in J\}.$$

(2) Το γινόμενο των I, J να είναι το

$$IJ = \{r \in R : \text{υπάρχει } n \in \mathbb{N}, a_1, \dots, a_n \in I, b_1, \dots, b_n \in J \text{ ώστε } r = a_1b_1 + \dots + a_nb_n\}.$$

Παρατηρήσεις 2.4.7

(α) $I, J \subseteq I + J$.

Πράγματι, εάν $a \in I$, τότε, επειδή $0_R \in J$, έχουμε $a = a + 0_R \in I + J$. Άρα $I \subseteq I + J$.

Ομοίως, $J \subseteq I + J$.

(β) $IJ \subseteq I \cap J$.

Πράγματι, έστω $r \in IJ$. Τότε υπάρχουν $n \in \mathbb{N}$, $a_1, \dots, a_n \in I$, $b_1, \dots, b_n \in J$ ώστε $r = a_1b_1 + \dots + a_nb_n$.

Επειδή το I είναι ιδεώδες, $a_1, \dots, a_n \in I$ και $b_1, \dots, b_n \in R$, έχουμε $a_1b_1, \dots, a_nb_n \in I$. Εφόσον το I είναι υποδακτύλιος, έπεται ότι $a_1b_1 + \dots + a_nb_n \in I$, δηλαδή $r \in I$. Αναλόγως δείχνουμε ότι $r \in J$. Άρα $r \in I \cap J$.

Πρόταση 2.4.8.

Έστω R δακτύλιος, I, J ιδεώδη του R . Τότε

(1) Το $I \cap J$ είναι ιδεώδες.

(2) Το $I + J$ είναι ιδεώδες.

(3) Το IJ είναι ιδεώδες.

Απόδειξη.

(1) Καταρχάς $0_R \in I \cap J$, αφού $0_R \in I$ και $0_R \in J$.

Έστω $a_1, a_2 \in I \cap J$ και $r \in R$. Εφόσον I, J είναι ιδεώδη, έχουμε $a_1 - a_2 \in I$, $ra_1, a_1r \in I$ και $a_1 - a_2 \in J$, $ra_1, a_1r \in J$. Άρα $a_1 - a_2, ra_1, a_1r \in I \cap J$.

(2) Καταρχάς $0_R = 0_R + 0_R \in I + J$.

Έστω $\delta_1, \delta_2 \in I + J$ και $r \in R$. Τότε υπάρχουν $a_1, a_2 \in I$, $b_1, b_2 \in J$ ώστε $\delta_1 = a_1 + b_1$, $\delta_2 = a_2 + b_2$.

Έχουμε

$$\delta_1 - \delta_2 = (a_1 - a_2) + (b_1 - b_2) \in I + J,$$

διότι $a_1 - a_2 \in I$ και $b_1 - b_2 \in J$.

Επίσης,

$$r\delta_1 = (ra_1) + (rb_1) \in I + J, \quad \delta_1r = (a_1r) + (b_1r) \in I + J,$$

διότι $ra_1, a_1r \in I$ και $rb_1, b_1r \in J$.

(3) Καταρχάς $0_R = 0_R \cdot 0_R \in IJ$.

Έστω $\omega_1, \omega_2 \in IJ$ και $r \in R$. Τότε υπάρχουν $n, m \in \mathbb{Z}^+$, $a_1, \dots, a_n, \gamma_1, \dots, \gamma_m \in I$ και $b_1, \dots, b_n, \delta_1, \dots, \delta_m \in J$ ώστε

$$\omega_1 = a_1b_1 + \dots + a_nb_n, \quad \omega_2 = \gamma_1\delta_1 + \dots + \gamma_m\delta_m.$$

Άρα

$$\omega_1 - \omega_2 = a_1 b_1 + \cdots + a_n b_n + (-\gamma_1)\delta_1 + \cdots + (-\gamma_m)\delta_m \in IJ,$$

διότι $-\gamma_1, \dots, -\gamma_m \in I$.

Επίσης,

$$r\omega_1 = (ra_1)b_1 + \cdots + (ra_n)b_n \in IJ,$$

διότι $ra_1, \dots, ra_n \in I$.

Ομοίως,

$$\omega_1 r = a_1(b_1 r) + \cdots + a_n(b_n r) \in IJ.$$

Παρατήρηση 2.4.9.

Η ένωση ιδεωδών δεν είναι πάντοτε ιδεώδες. Για παράδειγμα, στον $\mathbb{Z}$ έστω $I = \langle 2 \rangle$, $J = \langle 3 \rangle$. Αν το $I \cup J$ ήταν ιδεώδες, τότε, επειδή $2, 3 \in I \cup J$, θα είχαμε $5 = 2 + 3 \in I \cup J$. Άρα $5 \in I$ ή $5 \in J$, δηλαδή $2 \mid 5$ ή $3 \mid 5$, άτοπο.

Παραδείγματα 2.4.10

Έστω $I = \langle m \rangle$, $J = \langle n \rangle$ ιδεώδη του $\mathbb{Z}$, με $(m, n) \neq (0, 0)$. Τότε

(1) $I + J = \langle d \rangle$, όπου $d = \mu\kappa\delta(m, n)$.

(2) $I \cap J = \langle e \rangle$, όπου $e = \epsilon\kappa\pi(m, n)$.

(3) $IJ = \langle mn \rangle$.

Απόδειξη.

(1) Εφόσον $I = \{mx : x \in \mathbb{Z}\}$, $J = \{ny : y \in \mathbb{Z}\}$, έχουμε $I + J = \{mx + ny : x, y \in \mathbb{Z}\}$. Θέτουμε $d = \mu\kappa\delta(m, n)$. Από την ταυτότητα του Βézout υπάρχουν $x_0, y_0 \in \mathbb{Z}$ ώστε $d = mx_0 + ny_0 \in I + J$.

Άρα $d \in I + J$. Επειδή το $I + J$ είναι ιδεώδες του $\mathbb{Z}$, έχουμε $kd \in I + J$, για κάθε $k \in \mathbb{Z}$. Επομένως $\langle d \rangle \subseteq I + J$.

Αντίστροφα, έστω $t = mx + ny \in I + J$. Εφόσον $d \mid m$ και $d \mid n$, έχουμε $d \mid t$. Άρα $t \in \langle d \rangle$. Επομένως $I + J \subseteq \langle d \rangle$. Τελικά $I + J = \langle d \rangle$.

(2) Έχουμε ότι

$$k \in I \cap J \iff k \in I \text{ και } k \in J \iff m \mid k \text{ και } n \mid k \iff e \mid k \iff k \in \langle e \rangle.$$

Άρα $I \cap J = \langle e \rangle$.

(3) Καταρχάς, εφόσον $m \in I$ και $n \in J$, έχουμε $mn \in IJ$. Άρα $\langle mn \rangle \subseteq IJ$.

Αντίστροφα, έστω $t \in IJ$.

Τότε υπάρχουν $k \in \mathbb{N}$, $a_1, \dots, a_k \in I$, $b_1, \dots, b_k \in J$ ώστε

$$t = a_1 b_1 + \cdots + a_k b_k.$$

Για κάθε $i = 1, \dots, k$, εφόσον $m \mid a_i$ και $n \mid b_i$, έχουμε $mn \mid a_i b_i$.

Άρα $mn \mid (a_1 b_1 + \dots + a_k b_k)$, δηλαδή $t \in \langle mn \rangle$.

Επομένως $IJ = \langle mn \rangle$.

Πρόταση 2.4.11.

(α) Αν F σώμα, τότε τα μόνα ιδεώδη του F είναι τα τετριμμένα, δηλαδή τα $\{0_F\}, F$.

(β) Εάν R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο 1_R , τότε, εάν τα μόνα ιδεώδη του R είναι τα $\{0_R\}, R$, ο R είναι σώμα.

Απόδειξη.

(α) Έστω I ιδεώδες του F και έστω ότι $I \neq \{0_F\}$. Θα δείξουμε ότι $I = F$.

Έστω $a \in I$ με $a \neq 0_F$ (υπάρχει αφού $I \neq \{0_F\}$). Εφόσον $a \neq 0_F$ και ο F είναι σώμα, υπάρχει το a^{-1} .

Επειδή I ιδεώδες, $a \in I$ και $a^{-1} \in F$, έχουμε $a^{-1}a = 1_F \in I$.

Έστω τώρα $b \in F$. Εφόσον $1_F \in I$ και το I είναι ιδεώδες, $b = b1_F \in I$.

Άρα $F \subseteq I$. Εφόσον πάντοτε $I \subseteq F$, έπεται ότι $I = F$.

(β) Δεδομένου ότι ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, αρκεί να δείξουμε ότι κάθε $a \in R$ με $a \neq 0_R$ είναι αντιστρέψιμο.

Έστω λοιπόν $a \in R$ με $a \neq 0_R$ και θεωρούμε το κύριο ιδεώδες $I = \langle a \rangle$.

Εφόσον τα μόνα ιδεώδη του R είναι τα $\{0_R\}, R$, έχουμε $I = \{0_R\}$ ή $I = R$.

Επειδή όμως $a \in I$ και $a \neq 0_R$, έπεται ότι $I \neq \{0_R\}$. Άρα $I = R$, οπότε $1_R \in I$.

Εφόσον $I = \{ra : r \in R\}$, υπάρχει $r \in R$ ώστε $ra = 1_R$.

Άρα το a είναι αντιστρέψιμο, αφού, επειδή ο R είναι μεταθετικός, ισχύει και $ar = ra = 1_R$.

2.5 Χρήσιμα για συναρτήσεις

Ορισμός 2.5.1. 1-1 και επί συναρτήσεις

Έστω $\varphi : X \rightarrow Y$ συνάρτηση.

- Η φ λέγεται **1-1** εάν για κάθε $x_1, x_2 \in X$ ισχύει

$$\varphi(x_1) = \varphi(x_2) \implies x_1 = x_2.$$

Ισοδύναμα,

$$x_1 \neq x_2 \implies \varphi(x_1) \neq \varphi(x_2).$$

- Η φ λέγεται **επί** εάν το σύνολο τιμών της είναι όλο το Y , δηλαδή $\varphi(X) = Y$, ή ισοδύναμα, $\{\varphi(x) : x \in X\} = Y$.

Με άλλα λόγια, η φ είναι επί εάν για κάθε $y \in Y$ υπάρχει $x \in X$ τέτοιο ώστε $y = \varphi(x)$.

Παραδείγματα 2.5.2

1 Ναδειχθεί ότι η συνάρτηση $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 3x - 1$ είναι επί.

Λύση.

Πρέπει να δείξουμε ότι για κάθε $y \in \mathbb{R}$ υπάρχει $x \in \mathbb{R}$ ώστε $y = f(x) = 3x - 1$.

Έστω λοιπόν $y \in \mathbb{R}$. Θέλουμε να βρούμε $x \in \mathbb{R}$ ώστε $y = 3x - 1$.

Λύνοντας ως προς x , παίρνουμε $3x = y + 1 \iff x = \frac{y+1}{3}$.

Οπότε, για $x = \frac{y+1}{3}$ έχουμε $f(x) = 3 \cdot \frac{y+1}{3} - 1 = y$.

Άρα η f είναι επί.

2 Να εξετασθεί εάν η συνάρτηση $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ είναι επί.

Λύση.

Έχουμε $f(\mathbb{R}) = [0, +\infty) \neq \mathbb{R}$. Επομένως η f δεν είναι επί.

3 Να εξετασθεί εάν η συνάρτηση $f : \mathbb{R} \rightarrow [0, +\infty)$, $f(x) = x^2$ είναι επί.

Λύση.

Έχουμε $f(\mathbb{R}) = [0, +\infty)$. Άρα η f είναι επί.

4 Ναδειχθεί ότι η απεικόνιση $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, $\varphi(a) = [a]$, $a \in \mathbb{Z}$, είναι επί.

Λύση.

Έχουμε

$$\varphi(\mathbb{Z}) = \{\varphi(a) : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\} = \mathbb{Z}_n.$$

Άρα η φ είναι επί.

5 Ναδειχθεί ότι η συνάρτηση $f : \mathbb{C} \rightarrow \mathbb{C}$ με $f(z) = \bar{z}$, είναι επί.

Λύση.

Θα δείξουμε ότι για κάθε $w \in \mathbb{C}$ υπάρχει $z \in \mathbb{C}$ ώστε $f(z) = w$.

Έστω $w \in \mathbb{C}$. Θέτουμε $z = \bar{w}$.

Τότε $f(z) = \bar{z} = \overline{\bar{w}} = w$. Άρα η f είναι επί.

Ορισμός 2.5.3. Εικόνα και αντίστροφη εικόνα συνόλου

Έστω X, Y σύνολα, $f : X \rightarrow Y$ μία συνάρτηση και $A \subseteq X$, $B \subseteq Y$.

Την εικόνα του A μέσω της f ορίζουμε ως το σύνολο

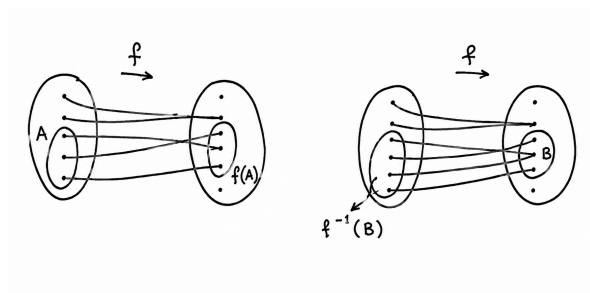
$$f(A) = \{f(x) : x \in A\}.$$

Την αντίστροφη εικόνα του B μέσω της f ορίζουμε ως το σύνολο

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Παρατήρηση 2.5.4.

Να μη συγχέουμε τον συμβολισμό $f^{-1}(B)$, που δηλώνει την αντίστροφη εικόνα του υποσυνόλου B του Y , με την αντίστροφη συνάρτηση.



Πρόταση 2.5.5. Βασικές ιδιότητες εικόνας και αντίστροφης εικόνας

Έστω $\varphi : X \rightarrow Y$ συνάρτηση, $A \subseteq X$ και $B \subseteq Y$.

(1) Ισχύει $\varphi^{-1}(\varphi(A)) \supseteq A$.

Απόδειξη.

Έστω $x \in A$. Τότε $\varphi(x) \in \varphi(A)$, άρα $x \in \varphi^{-1}(\varphi(A))$.

(2) Ισχύει $\varphi(\varphi^{-1}(B)) \subseteq B$.

Απόδειξη.

Έστω $y \in \varphi(\varphi^{-1}(B))$. Τότε υπάρχει $x \in \varphi^{-1}(B)$ ώστε $y = \varphi(x)$.

Επειδή $x \in \varphi^{-1}(B)$, έχουμε $\varphi(x) \in B$. Άρα $y \in B$.

(3) Αν η φ είναι 1-1, τότε $\varphi^{-1}(\varphi(A)) = A$.

Απόδειξη.

Από το (1) αρκεί να δείξουμε ότι $\varphi^{-1}(\varphi(A)) \subseteq A$.

Έστω $x \in \varphi^{-1}(\varphi(A))$. Τότε $\varphi(x) \in \varphi(A)$, οπότε υπάρχει $x_1 \in A$ ώστε $\varphi(x) = \varphi(x_1)$.

Επειδή η φ είναι 1-1, έχουμε $x = x_1$. Άρα $x \in A$.

(4) Αν η φ είναι επί, τότε $\varphi(\varphi^{-1}(B)) = B$.

Απόδειξη.

Από το (2) αρκεί να δείξουμε ότι $B \subseteq \varphi(\varphi^{-1}(B))$.

Έστω $y \in B$. Επειδή η φ είναι επί, υπάρχει $x \in X$ ώστε $y = \varphi(x)$.

Αφού $y \in B$, έχουμε $\varphi(x) \in B$, άρα $x \in \varphi^{-1}(B)$.

Επομένως $y = \varphi(x) \in \varphi(\varphi^{-1}(B))$.

2.6 Ομομορφισμοί δακτυλίων

Ορισμός 2.6.1.

Έστω R, S δύο δακτύλιοι και $\varphi : R \rightarrow S$ μία απεικόνιση.

Η φ θα καλείται **ομομορφισμός δακτυλίων** εάν για κάθε $r_1, r_2 \in R$,

$$(1) \quad \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \text{ και}$$

$$(2) \quad \varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2),$$

Επίσης, εάν επιπλέον

(α) η φ είναι επί, τότε καλείται **επιμορφισμός**.

(β) η φ είναι 1-1, τότε καλείται **μονομορφισμός**.

(γ) η φ είναι 1-1 και επί, τότε καλείται **ισομορφισμός**.

Παραδείγματα 2.6.2

(α) Εάν R, S δακτύλιοι, τότε η $\varphi : R \rightarrow S$ με

$$\varphi(r) = 0_S, \quad r \in R,$$

είναι ομομορφισμός δακτυλίων και καλείται ο **τετριμμένος ομομορφισμός** από τον R στον S .

(β) Εάν R δακτύλιος, τότε η ταυτοτική απεικόνιση $\varphi : R \rightarrow R$, με $\varphi(r) = r$, για κάθε $r \in R$, είναι ομομορφισμός δακτυλίων.

(γ) Έστω $n \in \mathbb{Z}^+$ με $n \geq 2$. Τότε η $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, με $\varphi(m) = [m]$, $m \in \mathbb{Z}$, είναι επιμορφισμός, όχι 1-1.

Πράγματι, καταρχάς παρατηρούμε ότι είναι ομομορφισμός, εφόσον, εάν $m, k \in \mathbb{Z}$, τότε

$$\varphi(m + k) = [m + k] = [m] + [k] = \varphi(m) + \varphi(k)$$

και

$$\varphi(mk) = [mk] = [m] \cdot [k] = \varphi(m)\varphi(k).$$

Επίσης, η φ είναι επί, αφού

$$\varphi(\mathbb{Z}) = \{\varphi(m) : m \in \mathbb{Z}\} = \{[m] : m \in \mathbb{Z}\} = \mathbb{Z}_n.$$

Τέλος, η φ δεν είναι 1-1, διότι

$$\varphi(0) = [0] = [n] = \varphi(n).$$

(δ) Έστω $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. Από το 12ο λυμένο γνωρίζουμε ότι το R είναι σώμα. Έστω $\varphi : R \rightarrow \mathbb{C}$, με

$$\varphi \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi, \quad a, b \in \mathbb{R}.$$

Η φ είναι ισομορφισμός.

Απόδειξη.

Καταρχάς η φ είναι ομομορφισμός.

$$\text{Έστω } r_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, r_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in R.$$

Τότε

$$\begin{aligned} \varphi(r_1 + r_2) &= (a_1 + a_2) + (b_1 + b_2)i \\ &= (a_1 + b_1i) + (a_2 + b_2i) \\ &= \varphi(r_1) + \varphi(r_2), \end{aligned}$$

και

$$\begin{aligned} \varphi(r_1 r_2) &= a_1 a_2 - b_1 b_2 + (a_1 b_2 + b_1 a_2)i \\ &= (a_1 + b_1i)(a_2 + b_2i) \\ &= \varphi(r_1) \varphi(r_2). \end{aligned}$$

Επίσης, η φ είναι επί. Πράγματι, εάν $z = a + bi \in \mathbb{C}$, τότε για $r = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in R$ έχουμε $\varphi(r) = z$.

Τέλος, η φ είναι 1-1. Πράγματι, εάν $\varphi(r_1) = \varphi(r_2)$, τότε $a_1 + b_1i = a_2 + b_2i \Rightarrow a_1 = a_2, b_1 = b_2 \Rightarrow r_1 = r_2$.

Άρα η φ είναι ισομορφισμός.

(ε) Η $\varphi : \mathbb{R} \rightarrow \mathbb{R}$, με $\varphi(a) = 2a, a \in \mathbb{R}$, δεν είναι ομομορφισμός δακτυλίων.

Πράγματι, εάν ήταν, τότε για $a_1 = a_2 = 1$ θα είχαμε

$$\varphi(a_1 a_2) = \varphi(a_1) \varphi(a_2) \Rightarrow \varphi(1) = (2 \cdot 1)(2 \cdot 1) \Rightarrow 2 = 4,$$

άτοπο.

(στ) Η $\varphi : \mathbb{C} \rightarrow \mathbb{R}$, με $\varphi(a + bi) = a, a + bi \in \mathbb{C}$, δεν είναι ομομορφισμός.

Πράγματι, εάν ήταν, τότε για $z_1 = z_2 = i$ θα είχαμε

$$\varphi(z_1 z_2) = \varphi(z_1) \varphi(z_2) \Rightarrow \varphi(-1) = \varphi(i) \varphi(i) \Rightarrow -1 = 0 \cdot 0 \Rightarrow -1 = 0,$$

άτοπο.

Πρόταση 2.6.3.

Έστω $\varphi : R \rightarrow S$ ομομορφισμός δακτυλίων. Τότε

- (1) $\varphi(0_R) = 0_S$.
- (2) $\varphi(-r) = -\varphi(r)$, για κάθε $r \in R$.
- (3) $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$, για κάθε $r_1, r_2 \in R$.
- (4) Για κάθε $r_1, \dots, r_n \in R$,

$$\varphi(r_1 + \dots + r_n) = \varphi(r_1) + \dots + \varphi(r_n)$$

και

$$\varphi(r_1 \cdots r_n) = \varphi(r_1) \cdots \varphi(r_n).$$

(5) Εάν $r \in R$, $k \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, τότε

$$\varphi(kr) = k\varphi(r) \quad \text{και} \quad \varphi(r^n) = (\varphi(r))^n.$$

Απόδειξη.

(1) Έχουμε

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R).$$

Προσθέτοντας και στα δύο μέλη το $-\varphi(0_R)$, παίρνουμε

$$0_S = \varphi(0_R) + (\varphi(0_R) - \varphi(0_R)) = \varphi(0_R),$$

δηλαδή $\varphi(0_R) = 0_S$.

(2) Έστω $r \in R$. Αρκεί να δείξουμε ότι ο αντίθετος του $\varphi(r)$ είναι ο $\varphi(-r)$.
Πράγματι,

$$\varphi(r) + \varphi(-r) = \varphi(r + (-r)) = \varphi(0_R) = 0_S,$$

όπου χρησιμοποιήσαμε το (1). Άρα $\varphi(-r) = -\varphi(r)$.

(3) Εάν $r_1, r_2 \in R$, τότε

$$\varphi(r_1 - r_2) = \varphi(r_1 + (-r_2)) = \varphi(r_1) + \varphi(-r_2) = \varphi(r_1) - \varphi(r_2).$$

(4) Με επαγωγή ως προς n .

(5) Έστω $k \in \mathbb{Z}$, $r \in R$.

Εάν $k > 0$, τότε

$$\varphi(kr) = \varphi(\underbrace{r + \cdots + r}_{k \text{ φορές}}) = \underbrace{\varphi(r) + \cdots + \varphi(r)}_{k \text{ φορές}} = k\varphi(r).$$

Εάν $k < 0$, τότε, επειδή $kr = (-k)(-r)$, έχουμε

$$\varphi(kr) = \varphi((-k)(-r)) = -k\varphi(-r) = -k(-\varphi(r)) = k\varphi(r).$$

Τέλος, εάν $k = 0$, τότε

$$\varphi(0r) = \varphi(0_R) = 0_S = 0\varphi(r).$$

Η σχέση $\varphi(r^n) = (\varphi(r))^n$ αποδεικνύεται με επαγωγή ως προς n .

Ορισμός 2.6.4. Πυρήνας και εικόνα ομομορφισμού

Έστω $\varphi : R \rightarrow S$ ομομορφισμός. Θέτουμε

(α) Τον πυρήνα του φ να είναι το υποσύνολο του R

$$\text{Ker } \varphi = \{r \in R : \varphi(r) = 0_S\}.$$

(β) Την εικόνα του φ να είναι το υποσύνολο του S

$$\text{Im } \varphi = \{\varphi(r) : r \in R\}$$

(δηλαδή το σύνολο τιμών του φ).

Πρόταση 2.6.5. (Ιδιότητες του πυρήνα)

Έστω $\varphi : R \rightarrow S$ ομομορφισμός. Τότε

(α) Ο $\text{Ker } \varphi$ είναι υποδακτύλιος του R .

(β) Ο $\text{Ker } \varphi$ είναι ιδεώδες του R .

(γ) $\text{Ker } \varphi = \{0_R\}$ αν και μόνο αν η φ είναι 1-1.

Απόδειξη.

(α) Καταρχάς $\text{Ker } \varphi \neq \emptyset$, αφού $\varphi(0_R) = 0_S$ (Πρόταση 2.6.3(1)), άρα $0_R \in \text{Ker } \varphi$.

Έστω $r_1, r_2 \in \text{Ker } \varphi$. Τότε $\varphi(r_1) = \varphi(r_2) = 0_S$. Επομένως $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = 0_S + 0_S = 0_S$ κι άρα $r_1 + r_2 \in \text{Ker } \varphi$.

Επίσης, $\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2) = 0_S 0_S = 0_S$, άρα $r_1 r_2 \in \text{Ker } \varphi$.

Τέλος, από την Πρόταση 2.6.3(2), $\varphi(-r_1) = -\varphi(r_1) = -0_S = 0_S$, άρα $-r_1 \in \text{Ker } \varphi$.

Οπότε ο $\text{Ker } \varphi$ είναι υποδακτύλιος του R .

(β) Έχουμε ήδη ότι $\text{Ker } \varphi \neq \emptyset$.

Εάν $r_1, r_2 \in \text{Ker } \varphi$, τότε

$$\varphi(r_1 - r_2) = \varphi(r_1 + (-r_2)) = \varphi(r_1) + (-\varphi(r_2)) = 0_S + (-0_S) = 0_S.$$

Άρα $r_1 - r_2 \in \text{Ker } \varphi$.

Επίσης, εάν $r \in R$ και $a \in \text{Ker } \varphi$, τότε

$$\varphi(ra) = \varphi(r) \varphi(a) = \varphi(r) 0_S = 0_S,$$

κι άρα $ra \in \text{Ker } \varphi$. Ομοίως, $ar \in \text{Ker } \varphi$.

Άρα ο $\text{Ker } \varphi$ είναι ιδεώδες του R .

(γ) ($\Rightarrow$) Έστω $r_1, r_2 \in R$ ώστε $\varphi(r_1) = \varphi(r_2)$. Τότε

$$\begin{aligned} \varphi(r_1) + (-\varphi(r_2)) &= 0_S \Rightarrow \varphi(r_1) + \varphi(-r_2) = 0_S \\ &\Rightarrow \varphi(r_1 + (-r_2)) = 0_S \end{aligned}$$

Άρα $r_1 + (-r_2) \in \text{Ker } \varphi$. Εφόσον $\text{Ker } \varphi = \{0_R\}$, έπεται ότι $r_1 + (-r_2) = 0_R$.

Άρα $(r_1 + (-r_2)) + r_2 = r_2$, οπότε $r_1 + ((-r_2) + r_2) = r_2$, δηλαδή $r_1 + 0_R = r_2$.

Άρα $r_1 = r_2$, επομένως η φ είναι 1-1.

($\Leftarrow$) Έστω $r \in \text{Ker } \varphi$. Τότε

$$\varphi(r) = 0_S \stackrel{(1)}{\Rightarrow} \varphi(r) = \varphi(0_R)$$

Εφόσον η φ είναι 1-1, έπεται ότι $r = 0_R$. Άρα $\text{Ker } \varphi = \{0_R\}$.

Πρόταση 2.6.6. (Ιδιότητες της εικόνας)

Έστω $\varphi : R \rightarrow S$ ομομορφισμός. Τότε

- (1) Η $\text{Im } \varphi$ είναι υποδακτύλιος του S .
- (2) Η φ είναι επί αν και μόνο αν $\text{Im } \varphi = S$.

Απόδειξη.

- (1) Καταρχάς προφανώς $\text{Im } \varphi \neq \emptyset$.

Έστω $s_1, s_2, s \in \text{Im } \varphi$. Τότε υπάρχουν $r_1, r_2, r \in R$ ώστε $s_1 = \varphi(r_1)$, $s_2 = \varphi(r_2)$, $s = \varphi(r)$.

Άρα $s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \text{Im } \varphi$.

Επίσης, $s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in \text{Im } \varphi$.

Τέλος, $-s = -\varphi(r) = \varphi(-r) \in \text{Im } \varphi$.

Άρα η $\text{Im } \varphi$ είναι υποδακτύλιος του S .

- (2) Προφανές, εφόσον $\text{Im } \varphi = \varphi(R)$.

Παρατήρηση 2.6.7.

Η $\text{Im } \varphi$ δεν είναι εν γένει ιδεώδες του S . Για παράδειγμα, έστω $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$ με $\varphi(n) = n$, $n \in \mathbb{Z}$. Η φ είναι ομομορφισμός, αλλά $\text{Im } \varphi = \varphi(\mathbb{Z}) = \mathbb{Z}$, το οποίο δεν είναι ιδεώδες του $\mathbb{Q}$.

Παρατήρηση 2.6.8. Μοναδιαίο και ομομορφισμοί

Έστω R, S δακτύλιοι ώστε ο R έχει μοναδιαίο στοιχείο και $\varphi : R \rightarrow S$ ομομορφισμός. Τότε

- (1) Το $\varphi(1_R)$ είναι μοναδιαίο της $\text{Im } \varphi$ και, εάν η φ είναι επί τότε και ο S έχει μοναδιαίο, το $\varphi(1_R)$.
- (2) Εάν η φ είναι επιμορφισμός και ο S έχει μοναδιαίο, τότε $\varphi(1_R) = 1_S$.
- (3) Εάν $\varphi(1_R) = 0_S$, τότε ο φ είναι τετριμμένος.
- (4) Εάν ο S έχει μοναδιαίο και ο φ δεν είναι τετριμμένος και $\varphi(1_R) \neq 1_S$, τότε το $\varphi(1_R)$ είναι μηδενοδιαίρετης του S .
- (5) Εάν ο S είναι ακέραια περιοχή και ο φ δεν είναι τετριμμένος, τότε $\varphi(1_R) = 1_S$.

Απόδειξη.

- (1) Αρκεί να δείξουμε ότι

$$s\varphi(1_R) = \varphi(1_R)s = s, \quad \text{για κάθε } s \in \text{Im } \varphi.$$

Έστω $s \in \text{Im } \varphi$. Τότε υπάρχει $r \in R$ με $s = \varphi(r)$.

Άρα

$$s\varphi(1_R) = \varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r) = s$$

και ομοίως $\varphi(1_R)s = s$.

(2) Από το (1) έχουμε ότι το $\varphi(1_R)$ είναι μοναδιαίο της $\text{Im } \varphi$ και, εφόσον η φ είναι επί, έχουμε $\text{Im } \varphi = S$. Άρα το $\varphi(1_R)$ είναι μοναδιαίο του S .

Γνωρίζουμε όμως ότι το μοναδιαίο σε έναν δακτύλιο (αν υπάρχει) είναι μοναδικό. Επομένως $\varphi(1_R) = 1_S$.

(3) Έστω $r \in R$. Τότε

$$\varphi(r) = \varphi(r1_R) = \varphi(r)\varphi(1_R) = \varphi(r)0_S = 0_S.$$

Άρα ο φ είναι τετριμμένος.

(4) Καταρχάς παρατηρούμε ότι $\varphi(1_R) \neq 0_S$, διότι, εάν $\varphi(1_R) = 0_S$, τότε από το (3) ο φ είναι τετριμμένος, άτοπο. Επίσης

$$\begin{aligned}\varphi(1_R) &= \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R) \Rightarrow \\ \varphi(1_R)\varphi(1_R) - \varphi(1_R) &= 0_S \Rightarrow \\ \varphi(1_R)\varphi(1_R) - \varphi(1_R)1_S &= 0_S \Rightarrow \\ \varphi(1_R)(\varphi(1_R) - 1_S) &= 0_S.\end{aligned}$$

Από υπόθεση $\varphi(1_R) \neq 1_S$, άρα $\varphi(1_R) - 1_S \neq 0_S$.

Επομένως $\varphi(1_R) \neq 0_S$ και $\varphi(1_R) - 1_S \neq 0_S$, ενώ

$$\varphi(1_R)(\varphi(1_R) - 1_S) = 0_S.$$

Άρα το $\varphi(1_R)$ είναι μηδενοδιαιρέτης του S . Μάλιστα, επειδή ισχύει και

$$(\varphi(1_R) - 1_S)\varphi(1_R) = \varphi(1_R)\varphi(1_R) - \varphi(1_R) = 0_S,$$

το $\varphi(1_R)$ είναι αριστερός και δεξιός μηδενοδιαιρέτης του S , ακόμη και όταν ο S δεν είναι μεταθετικός.

(5) Έχουμε $\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$. Άρα όπως πριν

$$\varphi(1_R)(\varphi(1_R) - 1_S) = 0_S.$$

Επειδή ο S είναι ακέραια περιοχή,

$$\varphi(1_R) = 0_S \quad \text{ή} \quad \varphi(1_R) - 1_S = 0_S.$$

Η πρώτη περίπτωση αποκλείεται από το (3), αφού τότε ο φ θα ήταν τετριμμένος. Άρα $\varphi(1_R) = 1_S$.

Παρατηρήσεις 2.6.9

(1) Εν γένει δεν ισχύει ότι, εάν $\varphi : R \rightarrow S$ ομομορφισμός και οι R, S έχουν μοναδιαία, τότε $\varphi(1_R) = 1_S$.

Για παράδειγμα, έστω $\varphi : \mathbb{Z} \rightarrow M_2(\mathbb{Z})$, με $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, για κάθε $a \in \mathbb{Z}$. Εύκολα η φ είναι ομομορφισμός. Επίσης $\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{M_2(\mathbb{Z})}$.

(2) Εάν $\varphi : R \rightarrow S$ ομομορφισμός και οι R, S έχουν μοναδιαία, τότε, όπως δείξαμε στα (2), (5),

εάν η φ είναι επί, τότε $\varphi(1_R) = 1_S$,

εάν ο S είναι ακέραια περιοχή και η φ δεν είναι τετριμμένη, τότε $\varphi(1_R) = 1_S$.

Πρόταση 2.6.10. Ομομορφισμοί και αντιστρέψιμα στοιχεία

Έστω R, S δακτύλιοι με μοναδιαία στοιχεία και $\varphi : R \rightarrow S$ ομομορφισμός.

(1) Αν $\varphi(1_R) = 1_S$, τότε, εάν $a \in U(R)$, έχουμε $\varphi(a) \in U(S)$ και άρα $\varphi(U(R)) \subseteq U(S)$.

(2) Αν η φ είναι επιμορφισμός, τότε $\varphi(U(R)) \subseteq U(S)$.

(3) Αν ο S είναι ακέραια περιοχή και η φ δεν είναι τετριμμένη, τότε $\varphi(U(R)) \subseteq U(S)$.

Απόδειξη.

(1) Έστω $a \in U(R)$. Τότε υπάρχει $b \in R$ ώστε $ab = ba = 1_R$. Οπότε

$$\varphi(ab) = \varphi(ba) = \varphi(1_R) = 1_S$$

και επομένως $\varphi(a)\varphi(b) = \varphi(b)\varphi(a) = 1_S$. Άρα η $\varphi(a)$ είναι αντιστρέψιμη και $(\varphi(a))^{-1} = \varphi(b) = \varphi(a^{-1})$. Συνεπώς $a \in U(R) \Rightarrow \varphi(a) \in U(S)$, δηλαδή $\varphi(U(R)) \subseteq U(S)$.

(2) Εάν η φ είναι επιμορφισμός, τότε από την Παρατήρηση 2.6.8(2) έχουμε ότι $\varphi(1_R) = 1_S$ και συνεπώς από το (1) έχουμε το ζητούμενο.

(3) Εάν ο S είναι ακέραια περιοχή και η φ δεν είναι τετριμμένη, τότε $\varphi(1_R) = 1_S$ (Παρατήρηση 2.6.8(5)) και συνεπώς από το (1) έπεται το ζητούμενο.

Παρατήρηση 2.6.11.

Εν γένει δεν ισχύει ότι $\varphi(U(R)) \subseteq U(S)$.

Για παράδειγμα, έστω $\varphi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ με $\varphi(a) = (a, 0)$, $a \in \mathbb{Z}$.

Το $1 \in U(\mathbb{Z})$, αλλά $\varphi(1) = (1, 0) \notin U(\mathbb{Z} \times \mathbb{Z})$, αφού

$$U(\mathbb{Z} \times \mathbb{Z}) = U(\mathbb{Z}) \times U(\mathbb{Z}) = \{(1, 1), (-1, 1), (1, -1), (-1, -1)\}.$$

Πρόταση 2.6.12. Ομομορφισμοί και μεταθετικότητα - μηδενοδιαιρέτες

Έστω $\varphi : R \rightarrow S$ ομομορφισμός, όπου R, S δακτύλιοι.

- (1) Αν η φ είναι επί και ο R μεταθετικός, τότε και ο S είναι μεταθετικός.
- (2) Αν η φ είναι 1-1 και το $a \in R$ είναι αριστερός (αντίστοιχα δεξιός) μηδενοδιαιρέτης του R , τότε το $\varphi(a)$ είναι αριστερός (αντίστοιχα δεξιός) μηδενοδιαιρέτης του S .

Απόδειξη.

- (1) Έστω $s_1, s_2 \in S$. Θα δείξουμε ότι $s_1 s_2 = s_2 s_1$.

Επειδή η φ είναι επί, υπάρχουν $r_1, r_2 \in R$ ώστε $s_1 = \varphi(r_1)$ και $s_2 = \varphi(r_2)$.

Οπότε

$$s_1 s_2 = \varphi(r_1) \varphi(r_2) = \varphi(r_1 r_2) = \varphi(r_2 r_1) = \varphi(r_2) \varphi(r_1) = s_2 s_1.$$

- (2) Έστω ότι το a είναι αριστερός μηδενοδιαιρέτης του R .

Τότε $a \neq 0_R$ και υπάρχει $b \in R$ με $b \neq 0_R$ ώστε $ab = 0_R$.

Παρατηρούμε ότι $\varphi(a) \neq 0_S$, διότι, αν $\varphi(a) = 0_S$, τότε $\varphi(a) = \varphi(0_R)$ και, επειδή η φ είναι 1-1, θα είχαμε $a = 0_R$, άτοπο.

Ομοίως $\varphi(b) \neq 0_S$.

Τέλος, επειδή $ab = 0_R$, έχουμε

$$\varphi(ab) = \varphi(0_R) \Rightarrow \varphi(a) \varphi(b) = 0_S.$$

Άρα ο $\varphi(a)$ είναι αριστερός μηδενοδιαιρέτης του S .

Η περίπτωση του δεξιού μηδενοδιαιρέτη αποδεικνύεται ανάλογα.

Άσκηση 1.

Να δοθούν παραδείγματα που να δείχνουν ότι δεν ισχύουν τα (1), (2) της Πρότασης 2.6.12 όταν η φ δεν είναι επί και όταν δεν είναι 1-1, αντίστοιχα.

Πρόταση 2.6.13.

Έστω R, S δακτύλιοι και $\varphi : R \rightarrow S$ ισομορφισμός. Τότε

- (1) Η $\varphi^{-1} : S \rightarrow R$ είναι ισομορφισμός.
- (2) Ο R είναι μεταθετικός αν και μόνο αν ο S είναι μεταθετικός.
- (3) Ο R έχει μοναδιαίο αν και μόνο αν ο S έχει μοναδιαίο.
- (4) Εάν οι R, S έχουν μοναδιαίο, τότε
 - i) $\varphi(1_R) = 1_S$,
 - ii) $r \in U(R)$ αν και μόνο αν $\varphi(r) \in U(S)$,
 - iii) $\varphi(U(R)) = U(S)$.
- (5) Εάν $r \in R$, τότε ο r είναι αριστερός (αντίστοιχα δεξιός) μηδενοδιαιρέτης του R αν και μόνο αν ο $\varphi(r)$ είναι αριστερός (αντίστοιχα δεξιός) μηδενοδιαιρέτης του S .

- (6) Ο R είναι ακέραια περιοχή αν και μόνο αν ο S είναι ακέραια περιοχή.
 (7) Ο R είναι σώμα αν και μόνο αν ο S είναι σώμα.

Απόδειξη.

(1) Η φ^{-1} προφανώς είναι 1-1 και επί.

Έστω $s_1, s_2 \in S$ και $r_1 = \varphi^{-1}(s_1)$, $r_2 = \varphi^{-1}(s_2)$.

Τότε

$$\varphi^{-1}(s_1 + s_2) = \varphi^{-1}(\varphi(r_1) + \varphi(r_2)) = \varphi^{-1}(\varphi(r_1 + r_2)) = r_1 + r_2 = \varphi^{-1}(s_1) + \varphi^{-1}(s_2).$$

Ομοίως,

$$\varphi^{-1}(s_1 s_2) = \varphi^{-1}(s_1) \varphi^{-1}(s_2).$$

Άρα η φ^{-1} είναι ισομορφισμός.

(2) $(\Rightarrow)$ Έστω ότι ο R είναι μεταθετικός. Η φ είναι επιμορφισμός, οπότε από την Πρόταση 2.6.12(1) έπεται ότι ο S είναι μεταθετικός.

$(\Leftarrow)$ Από το (1) έχουμε ότι η $\varphi^{-1} : S \rightarrow R$ είναι ισομορφισμός κι άρα επιμορφισμός. Επομένως, από την Πρόταση 2.6.12(1), επειδή ο S είναι μεταθετικός, έπεται ότι ο R είναι μεταθετικός.

(3) Αφήνεται ως άσκηση.

(4) i) Έπεται από την Παρατήρηση 2.6.8(2), αφού η φ είναι επί.

ii) $(\Rightarrow)$ Εάν $r \in U(R)$, τότε, από την Πρόταση 2.6.10(1), έχουμε $\varphi(r) \in U(S)$.

$(\Leftarrow)$ Εάν $\varphi(r) \in U(S)$, τότε, επειδή η φ^{-1} είναι ισομορφισμός, από το $(\Rightarrow)$ έχουμε $\varphi^{-1}(\varphi(r)) \in U(R)$, δηλαδή $r \in U(R)$.

iii) Από το ii) έχουμε αμέσως $\varphi(U(R)) = U(S)$.

(5) Αρκεί να αποδείξουμε την περίπτωση του αριστερού μηδενοδιαιρέτη.

$(\Rightarrow)$ Έπεται από την Πρόταση 2.6.12(2).

$(\Leftarrow)$ Εάν $\varphi(r)$ είναι αριστερός μηδενοδιαιρέτης του S , τότε, επειδή η φ^{-1} είναι ισομορφισμός, από το $(\Rightarrow)$ έχουμε ότι $\varphi^{-1}(\varphi(r)) = r$ είναι αριστερός μηδενοδιαιρέτης του R .

Ομοίως για δεξιούς μηδενοδιαιρέτες.

(6) $(\Rightarrow)$ Έστω ότι ο R είναι α.π. Θα δείξουμε ότι ο S είναι α.π.

Από το (2) έχουμε ότι ο S είναι μεταθετικός και από το (3) ότι ο S έχει μοναδιαίο στοιχείο. Επίσης, από το (4)i), $1_S = \varphi(1_R) \neq \varphi(0_R) = 0_S$, αφού $1_R \neq 0_R$ και η φ είναι 1-1.

Αρκεί να δείξουμε ότι ο S δεν έχει μηδενοδιαιρέτες.

Έστω $s \in S$ μηδενοδιαιρέτης του S . Τότε, επειδή η φ^{-1} είναι ισομορφισμός, από το (5) έχουμε ότι $\varphi^{-1}(s)$ είναι μηδενοδιαιρέτης του R , άτοπο, αφού ο R είναι α.π.

Άρα ο S δεν έχει μηδενοδιαιρέτες, οπότε είναι α.π.

($\Leftarrow$) Αν ο S είναι α.π., τότε εφαρμόζουμε το ($\Rightarrow$) στον ισομορφισμό $\varphi^{-1} : S \rightarrow R$ και παίρνουμε ότι ο R είναι α.π.

(7) ($\Rightarrow$) Έστω ότι ο R είναι σώμα. Θα δείξουμε ότι ο S είναι σώμα.

Από το (2) έχουμε ότι ο S είναι μεταθετικός και από το (3) ότι ο S έχει μοναδιαίο στοιχείο. Επίσης, από το (4)i), $1_S = \varphi(1_R) \neq \varphi(0_R) = 0_S$, αφού $1_R \neq 0_R$ και η φ είναι 1-1.

Έστω $s \in S$ με $s \neq 0_S$. Επειδή η φ είναι επί, υπάρχει $r \in R$ ώστε $s = \varphi(r)$.

Εφόσον $s \neq 0_S$, έχουμε $\varphi(r) \neq 0_S$, άρα $r \neq 0_R$. Επειδή ο R είναι σώμα, έχουμε $r \in U(R)$. Άρα, από το (4), $\varphi(r) \in U(S)$, δηλαδή $s \in U(S)$.

Επομένως ο S είναι σώμα.

($\Leftarrow$) Αν ο S είναι σώμα, τότε εφαρμόζουμε το ($\Rightarrow$) στον ισομορφισμό $\varphi^{-1} : S \rightarrow R$ και παίρνουμε ότι ο R είναι σώμα.

Ορισμός 2.6.14.

Έστω R, S δακτύλιοι. Θα λέμε ότι ο R είναι **ισόμορφος** με τον S , εάν υπάρχει ισομορφισμός $\varphi : R \rightarrow S$.

Θα γράφουμε $R \simeq S$, για να δηλώσουμε ότι ο R είναι ισόμορφος με τον S .

Πρόταση 2.6.15.

Έστω R, S, T τρεις δακτύλιοι. Τότε

- (1) $R \simeq R$.
- (2) Εάν $R \simeq S$, τότε $S \simeq R$.
- (3) Εάν $R \simeq S$ και $S \simeq T$, τότε $R \simeq T$.

Απόδειξη.

(1) Η ταυτοτική απεικόνιση $\varphi : R \rightarrow R$, με $\varphi(r) = r$, $r \in R$, είναι ισομορφισμός.

Άρα $R \simeq R$.

(2) Αν $\varphi : R \rightarrow S$ είναι ισομορφισμός, τότε, από την Πρόταση 2.6.13(1), η $\varphi^{-1} : S \rightarrow R$ είναι ισομορφισμός. Άρα $S \simeq R$.

(3) Έστω $\varphi : R \rightarrow S$ και $\psi : S \rightarrow T$ ισομορφισμοί.

Τότε η $\psi \circ \varphi : R \rightarrow T$ είναι ισομορφισμός (γιατί;). Άρα $R \simeq T$.

Πρόταση 2.6.16.

Έστω R, S ισόμορφοι δακτύλιοι. Τότε

- (1) Ο R έχει μοναδιαίο στοιχείο αν και μόνο αν ο S έχει μοναδιαίο στοιχείο.
- (2) Ο R είναι μεταθετικός αν και μόνο αν ο S είναι μεταθετικός.
- (3) Ο R έχει μηδενοδιαιρέτες αν και μόνο αν ο S έχει μηδενοδιαιρέτες.
- (4) Ο R είναι ακέραια περιοχή αν και μόνο αν ο S είναι ακέραια περιοχή.

(5) Ο R είναι σώμα αν και μόνο αν ο S είναι σώμα.

Απόδειξη.

Άμεσο από την Πρόταση 2.6.13.

2.7 Δακτύλιος πηλίκο

Ορισμός 2.7.1.

Έστω R δακτύλιος και I ιδεώδες του R .

Στον R ορίζουμε τη σχέση $\sim$ ως εξής:

$$\text{αν } a, b \in R, \text{ τότε } a \sim b \iff a - b \in I.$$

- Η $\sim$ είναι σχέση ισοδυναμίας (η απόδειξη αφήνεται ως άσκηση).

Εάν $a \in R$, τότε η κλάση ισοδυναμίας που αντιστοιχεί στο a είναι το σύνολο

$$[a] = \{a + x : x \in I\}.$$

[Πράγματι έχουμε ότι

$$\begin{aligned} [a] &= \{b \in R : b \sim a\} = \{b \in R : b - a \in I\} \\ &= \{b \in R : b - a = x \text{ για κάποιο } x \in I\} \\ &= \{b \in R : b = a + x \text{ για κάποιο } x \in I\} = \{a + x : x \in I\}.] \end{aligned}$$

- Την $[a]$ την συμβολίζουμε με $a + I$. Έχουμε λοιπόν

$$a + I = \{a + x : x \in I\}.$$

- Το σύνολο των κλάσεων ισοδυναμίας το συμβολίζουμε με R/I . Έχουμε λοιπόν

$$R/I = \{a + I : a \in R\}.$$

Παρατηρήσεις 2.7.2

(i) Εάν $a, b \in R$, τότε από τις ιδιότητες των κλάσεων ισοδυναμίας (1.6.4) έχουμε ότι

$$\text{είτε } a + I = b + I \iff a \sim b \iff a - b \in I,$$

$$\text{είτε } (a + I) \cap (b + I) = \emptyset \iff a \not\sim b \iff a - b \notin I.$$

(ii) Η κλάση ισοδυναμίας με αντιπρόσωπο το 0_R είναι το I εφόσον

$$0_R + I = \{0_R + x : x \in I\} = \{x : x \in I\} = I.$$

(iii) Εάν $a \in R$, τότε $a + I = I \iff a \in I$.

[Πράγματι, έχουμε ότι

$$a + I = I \iff a + I = 0_R + I \stackrel{(i)}{\iff} a - 0_R \in I \iff a \in I.]$$

(iv) Αν $I = R$, τότε $R/I = \{I\}$. (γιατί;)

Παράδειγμα 2.7.3.

Έστω $R = \mathbb{Z}$, $I = \langle n \rangle$ και $a, b \in \mathbb{Z}$. Τότε

$$a + I = b + I \iff a \equiv b \pmod{n}.$$

Πράγματι, έχουμε ότι

$$a + I = b + I \iff a - b \in I = \langle n \rangle \iff n \mid (a - b) \iff a \equiv b \pmod{n}.$$

Επίσης, εάν $a \in \mathbb{Z}$, τότε

$$\begin{aligned} a + I &= \{b \in \mathbb{Z} : b \sim a\} \\ &= \{b \in \mathbb{Z} : b - a \in I = \langle n \rangle\} \\ &= \{b \in \mathbb{Z} : n \mid (a - b)\} \\ &= \{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = [a]_n. \end{aligned}$$

Ορισμός 2.7.4. (Πράξεις στον R/I)

Στο R/I ορίζουμε τις πράξεις $+$, $\cdot$ ως εξής:

Εάν $a + I, b + I \in R/I$, τότε

$$(a + I) + (b + I) = (a + b) + I$$

και

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

• Οι πράξεις είναι καλά ορισμένες.

Πράγματι, αρκεί να δείξουμε ότι, εάν $a, a', b, b' \in R$ ώστε $a + I = a' + I$ και $b + I = b' + I$, τότε $(a + b) + I = (a' + b') + I$ και $ab + I = a'b' + I$.

Έστω λοιπόν $a, a', b, b' \in R$ με $a + I = a' + I$ και $b + I = b' + I$.

Τότε $a - a', b - b' \in I$. Επειδή το I είναι ιδεώδες, έχουμε $(a - a') + (b - b') \in I$, οπότε $(a + b) - (a' + b') \in I$. Άρα $(a + b) + I = (a' + b') + I$.

Επίσης, επειδή το I είναι ιδεώδες, $a - a' \in I$, $b \in R$, έχουμε $(a - a')b \in I$, δηλαδή $ab - a'b \in I$. (1)

Ανάλογα, $a' \in R$, $b - b' \in I$, άρα $a'(b - b') \in I$, δηλαδή $a'b - a'b' \in I$. (2)

Από τις (1), (2), επειδή το I είναι υποδακτύλιος, έχουμε $ab - a'b + a'b - a'b' = ab - a'b' \in I$.

Άρα $ab + I = a'b' + I$.

Πρόταση 2.7.5.

(1) Ο R/I , εφοδιασμένος με τις παραπάνω πράξεις, είναι δακτύλιος και ονομάζεται **δακτύλιος πηλίκο**. Επίσης, $0_{R/I} = 0_R + I = I$.

(2) Αν ο R είναι μεταθετικός, τότε και ο R/I είναι μεταθετικός.

(3) Αν ο R έχει μοναδιαίο στοιχείο 1_R , τότε το $1_R + I$ είναι το μοναδιαίο του R/I .

Απόδειξη.

(1) Πρέπει να δείξουμε ότι ισχύουν τα αξιώματα του δακτυλίου.

Έστω $a + I, b + I, c + I \in R/I$.

Έχουμε

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

Ομοίως,

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

Επίσης,

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

Το ουδέτερο στοιχείο ως προς την πρόσθεση είναι το

$$0_R + I = I,$$

διότι

$$(a + I) + I = (a + 0_R) + I = a + I.$$

Ο αντίθετος του $a + I$ είναι το $(-a) + I$, αφού

$$(a + I) + ((-a) + I) = (a - a) + I = 0_R + I = I.$$

Τέλος,

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

Ομοίως αποδεικνύεται και η δεξιά επιμεριστική ιδιότητα.

Άρα ο R/I είναι δακτύλιος.

(2) Εάν ο R είναι μεταθετικός, τότε

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

για κάθε $a + I, b + I \in R/I$.

Άρα ο R/I είναι μεταθετικός.

(3) Έστω ότι ο R έχει μοναδιαίο στοιχείο 1_R .

Τότε, για κάθε $a + I \in R/I$,

$$(1_R + I)(a + I) = 1_R a + I = a + I$$

και

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

Άρα το $1_R + I$ είναι το μοναδιαίο στοιχείο του R/I .

Θεώρημα 2.7.6. Πρώτο Θεώρημα Ισομορφισμού Δακτυλίων (1ο Θ.Ι.Δ.)

Έστω R, S δακτύλιοι και $\varphi : R \rightarrow S$ ομομορφισμός. Τότε

$$R/\text{Ker } \varphi \simeq \text{Im } \varphi.$$

Απόδειξη.

Έστω $\overline{\varphi} : R/\text{Ker } \varphi \rightarrow \text{Im } \varphi$ με

$$\overline{\varphi}(a + \text{Ker } \varphi) = \varphi(a).$$

Η $\overline{\varphi}$ είναι καλά ορισμένη.

Πράγματι, έστω $a, b \in R$ ώστε $a + \text{Ker } \varphi = b + \text{Ker } \varphi$.

Τότε $a - b \in \text{Ker } \varphi$, άρα $\varphi(a - b) = 0_S$, δηλαδή $\varphi(a) = \varphi(b)$.

Επομένως $\overline{\varphi}(a + \text{Ker } \varphi) = \overline{\varphi}(b + \text{Ker } \varphi)$.

Η $\overline{\varphi}$ είναι ομομορφισμός.

Πράγματι έστω $a + \text{Ker } \varphi, b + \text{Ker } \varphi \in R/\text{Ker } \varphi$.

Τότε

$$\begin{aligned}\overline{\varphi}((a + \text{Ker } \varphi) + (b + \text{Ker } \varphi)) &= \overline{\varphi}(a + b + \text{Ker } \varphi) \\ &= \varphi(a + b) \\ &= \varphi(a) + \varphi(b) \\ &= \overline{\varphi}(a + \text{Ker } \varphi) + \overline{\varphi}(b + \text{Ker } \varphi).\end{aligned}$$

Ομοίως,

$$\begin{aligned}\overline{\varphi}((a + \text{Ker } \varphi)(b + \text{Ker } \varphi)) &= \overline{\varphi}(ab + \text{Ker } \varphi) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \overline{\varphi}(a + \text{Ker } \varphi)\overline{\varphi}(b + \text{Ker } \varphi).\end{aligned}$$

Η $\bar{\varphi}$ είναι 1-1

Πράγματι αν $a + \text{Ker } \varphi, b + \text{Ker } \varphi \in R / \text{Ker } \varphi$ ώστε $\bar{\varphi}(a + \text{Ker } \varphi) = \bar{\varphi}(b + \text{Ker } \varphi)$.
Τότε

$$\varphi(a) = \varphi(b) \Rightarrow \varphi(a - b) = 0_S \Rightarrow a - b \in \text{Ker } \varphi \Rightarrow a + \text{Ker } \varphi = b + \text{Ker } \varphi.$$

Η $\bar{\varphi}$ είναι επί.

Έστω $s \in \text{Im } \varphi$. Τότε υπάρχει $a \in R$ ώστε $s = \varphi(a)$. Άρα

$$\bar{\varphi}(a + \text{Ker } \varphi) = \varphi(a) = s.$$

Επομένως η $\bar{\varphi}$ είναι ισομορφισμός και συνεπώς

$$R / \text{Ker } \varphi \simeq \text{Im } \varphi.$$

Παράδειγμα 2.7.7.

Έστω $n \in \mathbb{Z}, n > 0$. Να αποδειχθεί ότι $\mathbb{Z}/I \simeq \mathbb{Z}_n$, όπου $I = \langle n \rangle$.

Λύση.

Έστω η απεικόνιση $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ με $\varphi(k) = [k], k \in \mathbb{Z}$.

Η φ είναι ομομορφισμός (Γιατί;).

Επίσης η φ είναι επί, εφόσον

$$\text{Im } \varphi = \{\varphi(k) : k \in \mathbb{Z}\} = \{[k] : k \in \mathbb{Z}\} = \mathbb{Z}_n.$$

Τέλος, $\text{Ker } \varphi = I$, εφόσον, εάν $k \in \mathbb{Z}$, τότε

$$\begin{aligned} k \in \text{Ker } \varphi &\iff \varphi(k) = [0] \iff [k] = [0] \\ &\iff n \mid k \iff k \in \langle n \rangle = I. \end{aligned}$$

Επίσης από το 1ο Θεώρημα Ισομορφισμού Δακτυλίων, έχουμε ότι

$$\mathbb{Z} / \text{Ker } \varphi \simeq \text{Im } \varphi,$$

και εφόσον $\text{Im } \varphi = \mathbb{Z}_n$ και $\text{Ker } \varphi = I$, έπεται ότι $\mathbb{Z}/I \simeq \mathbb{Z}_n$.

Παρατήρηση 2.7.8.

Στην πραγματικότητα δεν ισχύει απλώς $\mathbb{Z}/I \simeq \mathbb{Z}_n$, αλλά $\mathbb{Z}/I = \mathbb{Z}_n$.

Πράγματι, εάν $a \in \mathbb{Z}$, τότε $a + I = \{a + kn : k \in \mathbb{Z}\} = [a]$ εφόσον εάν $b \in \mathbb{Z}$ τότε

$$b \in a + I \iff b - a \in I \iff \exists k \in \mathbb{Z} : b = a + kn.$$

Άρα

$$\mathbb{Z}/I = \{a + I : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\} = \mathbb{Z}_n.$$

2.8 Κινέζικο Θεώρημα Υπολοίπων

Θεώρημα 2.8.1. Κινέζικο Θεώρημα Υπολοίπων (Κ.Θ.Υ.)

Έστω R δακτύλιος και I, J ιδεώδη του R ώστε $I + J = R$. Τότε

$$R/(I \cap J) \simeq (R/I) \times (R/J).$$

Απόδειξη.

Έστω

$$\varphi : R \longrightarrow (R/I) \times (R/J), \quad \varphi(r) = (r + I, r + J), \quad r \in R.$$

Θα δείξουμε ότι

(i) $\text{Ker } \varphi = I \cap J$.

(ii) Η φ είναι επί.

Οπότε, από το 1ο Θεώρημα Ισομορφισμού, θα έχουμε ότι

$$R/\text{Ker } \varphi \simeq \text{Im } \varphi \xrightarrow{\text{Ker } \varphi = I \cap J, \varphi \text{ επί}} R/(I \cap J) \simeq (R/I) \times (R/J).$$

Για το (i) έχουμε. Έστω $r \in R$. Τότε

$$\begin{aligned} r \in \text{Ker } \varphi &\iff \varphi(r) = 0_{R/I \times R/J} \\ &\iff (r + I, r + J) = (I, J) \\ &\iff r + I = I \text{ και } r + J = J \\ &\iff r \in I \text{ και } r \in J \\ &\iff r \in I \cap J. \end{aligned}$$

Για το (ii) έχουμε. Έστω $(r_1 + I, r_2 + J) \in (R/I) \times (R/J)$.

Θέλουμε να δείξουμε ότι υπάρχει $r \in R$ ώστε

$$\varphi(r) = (r_1 + I, r_2 + J) \iff (r + I, r + J) = (r_1 + I, r_2 + J).$$

Δηλαδή πρέπει να δείξουμε ότι, για τυχόν $r_1, r_2 \in R$, υπάρχει $r \in R$ ώστε

$$r + I = r_1 + I \quad \text{και} \quad r + J = r_2 + J$$

$$\iff r - r_1 \in I \quad \text{και} \quad r - r_2 \in J.$$

Έστω λοιπόν $r_1, r_2 \in R$.

Εφόσον $r_1, r_2 \in R$ και $I + J = R$, υπάρχουν $x_1, x_2 \in I$, $y_1, y_2 \in J$ ώστε

$$r_1 = x_1 + y_1 \quad \text{και} \quad r_2 = x_2 + y_2.$$

Θέτουμε

$$x = x_2 - x_1 \in I, \quad y = y_1 - y_2 \in J \quad \text{και} \quad r = y_1 + x_2.$$

Τότε

$$r - r_1 = y_1 + x_2 - x_1 - y_1 = x_2 - x_1 = x \in I$$

και

$$r - r_2 = y_1 + x_2 - x_2 - y_2 = y_1 - y_2 = y \in J.$$

Επομένως η φ είναι επί.

Παραδείγματα 2.8.2

(α) Έστω $m, n \in \mathbb{Z}$, $m, n > 1$, με $(m, n) = 1$. Τότε

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$

Απόδειξη.

Έστω $I = \langle m \rangle$ και $J = \langle n \rangle$. Παρατηρούμε ότι

(i) $I + J = \mathbb{Z}$.

Πράγματι, προφανώς $I + J \subseteq \mathbb{Z}$ κι άρα πρέπει να δείξουμε ότι $\mathbb{Z} \subseteq I + J$.

Εφόσον $(m, n) = 1$, υπάρχουν $k, \lambda \in \mathbb{Z}$ ώστε $km + \lambda n = 1$. (1)

Έστω $a \in \mathbb{Z}$. Από την (1) πολλαπλασιάζοντας με a έχουμε

$$(ak)m + (a\lambda)n = a.$$

Θέτοντας $x = (ak)m$ και $y = (a\lambda)n$, έχουμε ότι $x \in I$, $y \in J$ και $a = x + y$.

Οπότε $a \in I + J$. Άρα $\mathbb{Z} \subseteq I + J$

(ii) $I \cap J = \langle mn \rangle$.

Πράγματι καταρχάς από το Παράδειγμα 2.4.10(2) έχουμε ότι $I \cap J = \langle \ell \rangle$, όπου $\ell = \text{εκπ}(m, n)$. Επίσης οι m, n είναι σχετικά πρώτοι, κι άρα $\ell = mn$.

(iii) Από το Κ.Θ.Υ. έχουμε ότι

$$\mathbb{Z}/(I \cap J) \simeq (\mathbb{Z}/I) \times (\mathbb{Z}/J).$$

Επίσης, από το παράδειγμα 2.7.7 έχουμε ότι

$$\mathbb{Z}/(I \cap J) \simeq \mathbb{Z}_{mn}, \quad \mathbb{Z}/I \simeq \mathbb{Z}_m, \quad \mathbb{Z}/J \simeq \mathbb{Z}_n.$$

Οπότε

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$

(Κοίτα επίσης εάν θες το 62ο λυμένο για απευθείας απόδειξη.)

(β) (Γενίκευση του (α))

Έστω $m_1, m_2, \dots, m_k$ k -ακέραιοι ανά δύο σχετικά πρώτοι.

Τότε

$$\mathbb{Z}_{m_1 m_2 \dots m_k} \simeq \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}.$$

(Με επαγωγή στο k .)

2.9 Πρώτα και μεγιστικά ιδεώδη

Ορισμός 2.9.1.

Έστω R δακτύλιος και $I \subseteq R$ ένα ιδεώδες του R . Τότε

(α) Το I θα καλείται **πρώτο ιδεώδες** εάν

(i) $I \neq R$ και (ii) Για κάθε $a, b \in R$, εάν $ab \in I$, τότε $a \in I$ ή $b \in I$.

(β) Το I θα καλείται **μεγιστικό ιδεώδες** εάν

(i) $I \neq R$ και (ii) Εάν J είναι ιδεώδες του R με $I \subseteq J$, τότε $J = I$ ή $J = R$.

(Δηλαδή τα μοναδικά ιδεώδη του R που περιέχουν το I , είναι το I και το R .)

Παραδείγματα 2.9.2

(1) Εάν R είναι α.π., τότε το $I = \{0_R\}$ είναι πρώτο ιδεώδες.

Πράγματι, εάν $a, b \in R$ με $ab \in I$, τότε $ab = 0_R$. Εφόσον ο R είναι α.π., έχουμε $a = 0_R$ ή $b = 0_R$, δηλαδή $a \in I$ ή $b \in I$.

(2) Εάν F είναι σώμα, τότε το $I = \{0_F\}$ είναι μεγιστικό ιδεώδες. (Γιατί;)

(3) Έστω I ιδεώδες του $\mathbb{Z}$ με $I \neq \{0\}, \mathbb{Z}$. Ως γνωστόν υπάρχει $n \in \mathbb{Z}_{>0}$ με $I = \langle n \rangle$.
Ισχύει ότι

Το I είναι πρώτο αν και μόνο αν ο n είναι πρώτος.

Απόδειξη.

($\Leftarrow$) Έστω $a, b \in \mathbb{Z}$ με $ab \in I = \langle n \rangle$. Τότε $n \mid ab$.

Εφόσον ο n είναι πρώτος, $n \mid a$ ή $n \mid b$.

Άρα $a \in I$ ή $b \in I$.

($\Rightarrow$) Έστω ότι ο n δεν είναι πρώτος.

Τότε υπάρχουν $a, b \in \mathbb{Z}$ με $1 < a, b < n$ ώστε $n = ab$.

Γι' αυτούς τους a, b έχουμε $ab = n \in I$, αλλά προφανώς $a, b \notin I$, αφού $1 < a, b < n$.

Άτοπο, επειδή το I είναι πρώτο.

Άρα ο n είναι πρώτος.

(4) Έστω I ιδεώδες του $\mathbb{Z}$ με $I \neq \{0\}, \mathbb{Z}$.

Τότε το I είναι μεγιστικό ιδεώδες αν και μόνο αν υπάρχει p πρώτος αριθμός ώστε $I = \langle p \rangle$.

Απόδειξη.

($\Rightarrow$) Εφόσον $I \neq \{0\}$, υπάρχει $d \in \mathbb{Z}_{>0}$ ώστε $I = \langle d \rangle$. Επίσης εφόσον $I \neq \mathbb{Z}$ έχουμε ότι $1 < d$. Θα δείξουμε ότι ο d είναι πρώτος. Έστω προς άτοπο ότι δεν είναι πρώτος.

Τότε υπάρχει $1 < a < d$ ώστε $a \mid d$. Θέτουμε $J = \langle a \rangle$.

Τότε $I \subseteq J$, $J \neq I$ (αφού $a \in J$, $a \notin I$) και $J \neq \mathbb{Z}$ (αφού $a > 1$).

Άτοπο, διότι το I είναι μεγιστικό.

($\Leftarrow$) Έστω τώρα $I = \langle p \rangle$, όπου p πρώτος. Έστω J ιδεώδες του $\mathbb{Z}$ με $I \subseteq J$.

Εφόσον το J είναι ιδεώδες του $\mathbb{Z}$, υπάρχει $n \in \mathbb{Z}_{\geq 0}$ ώστε $J = \langle n \rangle$.

Από $\langle p \rangle \subseteq \langle n \rangle$ έπεται ότι $p \in \langle n \rangle$, δηλαδή $n \mid p$.

Επειδή ο p είναι πρώτος, $n = 1$ ή $n = p$.

Άρα $J = \mathbb{Z}$ ή $J = \langle p \rangle = I$. Επομένως το I είναι μεγιστικό ιδεώδες.

β' τρόπος για το αντίστροφο (χωρίς χρήση του γεγονότος ότι κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο).

($\Leftarrow$) Έστω J ιδεώδες του $\mathbb{Z}$ με $I \subseteq J$.

Έστω ότι $J \neq I$. Τότε υπάρχει $n \in J$ με $n \notin I$.

Επειδή $I = \langle p \rangle$, έχουμε $p \nmid n$. Εφόσον ο p είναι πρώτος, $(p, n) = 1$.

Άρα υπάρχουν $x, y \in \mathbb{Z}$ ώστε $xp + yn = 1$.

Εφόσον $p \in I \subseteq J$, $n \in J$ και το J είναι ιδεώδες, έχουμε $xp + yn = 1 \in J$.

Άρα $J = \mathbb{Z}$. Επομένως $J = I$ ή $J = \mathbb{Z}$, δηλαδή το I είναι μεγιστικό ιδεώδες.

Θεώρημα 2.9.3.

Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και I ιδεώδες του R με $I \neq R$. Τότε

(1) Το I είναι πρώτο αν και μόνο αν ο R/I είναι ακέραιο περιοχή.

(2) Το I είναι μεγιστικό αν και μόνο αν ο R/I είναι σώμα.

Απόδειξη.

(1) ($\Rightarrow$) Εφόσον ο R είναι μεταθετικός, ο R/I είναι μεταθετικός. Επίσης, το μοναδιαίο του R/I είναι το $1_R + I$ και $1_R + I \neq 0_{R/I} = I$, αφού $I \neq R$. Άρα αρκεί να δείξουμε ότι ο R/I δεν έχει μηδενοδιαιρέτες.

Έστω $a + I, b + I \in R/I$ με $(a + I)(b + I) = 0_{R/I} = I$.

Τότε $ab + I = I$, άρα $ab \in I$. Επειδή το I είναι πρώτο, έχουμε $a \in I$ ή $b \in I$, οπότε $a + I = I$ ή $b + I = I$. Άρα ο R/I είναι ακέραιο περιοχή.

($\Leftarrow$) Έστω $a, b \in R$ με $ab \in I$. Τότε $(a + I)(b + I) = ab + I = I = 0_{R/I}$.

Επειδή ο R/I είναι ακέραιο περιοχή, έχουμε $a + I = I$ ή $b + I = I$, άρα $a \in I$ ή $b \in I$. Επομένως το I είναι πρώτο.

(2) ($\Rightarrow$) Εφόσον ο R είναι μεταθετικός με μοναδιαίο στοιχείο, ο R/I είναι μεταθετικός με μοναδιαίο το $1_R + I$. Επίσης, $1_R + I \neq 0_{R/I} = I$, αφού $I \neq R$. Αρκεί λοιπόν να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R/I είναι αντιστρέψιμο.

Έστω $a + I \in R/I$ με $a + I \neq 0_{R/I} = I$. Εφόσον $a + I \neq I$, έχουμε $a \notin I$.

Θέτουμε $J = \{b + ra : b \in I, r \in R\} = I + \langle a \rangle$.

Από την Πρόταση 2.4.8(2), το J είναι ιδεώδες του R . Επίσης $I \subseteq J$, αφού, εάν $b \in I$, τότε $b = b + 0_R a \in J$.

Επειδή το I είναι μεγιστικό, έχουμε $J = I$ ή $J = R$. Όμως $J \neq I$, αφού $a \in J$ και $a \notin I$. Άρα $J = R$.

Επομένως $1_R \in J$, οπότε υπάρχουν $b \in I$ και $r \in R$ ώστε $b + ra = 1_R$. Άρα

$$(b + ra) + I = 1_R + I \Rightarrow (b + I) + (ra + I) = 1_R + I \Rightarrow (r + I)(a + I) = 1_R + I.$$

Επειδή ο R/I είναι μεταθετικός, έχουμε και $(a + I)(r + I) = 1_R + I$. Άρα το $a + I$ είναι αντιστρέψιμο και επομένως ο R/I είναι σώμα.

($\Leftarrow$) Έστω J ιδεώδες του R με $I \subseteq J$. Θα δείξουμε ότι $J = I$ ή $J = R$.

Έστω ότι $J \neq I$. Τότε υπάρχει $a \in J$ με $a \notin I$. Άρα $a + I \neq I = 0_{R/I}$.

Επειδή ο R/I είναι σώμα, υπάρχει $r + I \in R/I$ ώστε $(a + I)(r + I) = 1_R + I$.

Επομένως $ar + I = 1_R + I$, άρα $1_R - ar \in I$. Εφόσον $I \subseteq J$, έχουμε $1_R - ar \in J$.

Επίσης, επειδή $a \in J$ και το J είναι ιδεώδες, έχουμε $ar \in J$.

Άρα $1_R = (1_R - ar) + ar \in J$, οπότε $J = R$.

Επομένως $J = I$ ή $J = R$, άρα το I είναι μεγιστικό.

Πόρισμα 2.9.4.

Εάν R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, τότε κάθε μεγιστικό ιδεώδες του R είναι και πρώτο.

Απόδειξη.

Έστω I μεγιστικό ιδεώδες του R .

Από το Θεώρημα 2.9.3 έχουμε ότι ο R/I είναι σώμα.

Επομένως ο R/I είναι ακέραια περιοχή.

Άρα, πάλι από το Θεώρημα 2.9.3, το I είναι πρώτο ιδεώδες.

Παραδείγματα 2.9.5

(α) Έστω $R = \mathbb{Z}_6$, $I = \langle [3] \rangle = \{[0], [3]\}$.

Παρατηρούμε ότι

$$\mathbb{Z}_6/I = \{I, [1] + I, [2] + I\}.$$

Επίσης, η απεικόνιση $\varphi : \mathbb{Z}_6/I \rightarrow \mathbb{Z}_3$ με

$$\varphi(I) = [0]_3, \quad \varphi([1] + I) = [1]_3, \quad \varphi([2] + I) = [2]_3$$

είναι ισομορφισμός δακτυλίων. (Γιατί;)

Άρα ο $\mathbb{Z}_6/I$ είναι σώμα (εφόσον ο $\mathbb{Z}_3$ είναι σώμα) και συνεπώς το I είναι μεγιστικό ιδεώδες του $\mathbb{Z}_6$.

Αξίζει να παρατηρήσουμε ότι, παρόλο που ο $\mathbb{Z}_6$ δεν είναι ακέραια περιοχή, ο $\mathbb{Z}_6/I$ είναι σώμα.

(β) Έστω $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(0, n) : n \in \mathbb{Z}\}$.

Το I είναι ιδεώδες του R .

Επίσης, η απεικόνιση $\varphi : (\mathbb{Z} \times \mathbb{Z})/I \rightarrow \mathbb{Z}$ με

$$\varphi((m, n) + I) = m$$

είναι ισομορφισμός δακτυλίων.

Πράγματι, η φ είναι καλά ορισμένη, διότι εάν $(m_1, n_1) + I = (m_2, n_2) + I$, τότε $(m_1 - m_2, n_1 - n_2) \in I$, οπότε $m_1 - m_2 = 0$, δηλαδή $m_1 = m_2$.

Είναι προφανώς ομομορφισμός.

Επίσης είναι 1-1, αφού

$$\varphi((m, n) + I) = 0 \iff m = 0 \iff (m, n) \in I \iff (m, n) + I = I = 0_{(\mathbb{Z} \times \mathbb{Z})/I}.$$

Τέλος, είναι επί, αφού για κάθε $m \in \mathbb{Z}$,

$$\varphi((m, 0) + I) = m.$$

Άρα

$$(\mathbb{Z} \times \mathbb{Z})/I \simeq \mathbb{Z}.$$

Εφόσον ο $\mathbb{Z}$ είναι ακέραια περιοχή, από το Θεώρημα 2.9.3 έπεται ότι το I είναι πρώτο ιδεώδες.

Το I δεν είναι μεγιστικό, διότι αν ήταν, τότε από το Θεώρημα 2.9.3 ο $(\mathbb{Z} \times \mathbb{Z})/I$ θα ήταν σώμα. Εφόσον όμως

$$(\mathbb{Z} \times \mathbb{Z})/I \simeq \mathbb{Z},$$

θα έπρεπε ο $\mathbb{Z}$ να είναι σώμα, άτοπο.

Άσκηση 2.

Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και I ιδεώδες του R .

Ναδειχθεί ότι, εάν ο R/I είναι ακέραια περιοχή και περιέχει μη μηδενικό στοιχείο που δεν είναι αντιστρέψιμο, τότε το I είναι πρώτο αλλά όχι μεγιστικό.

Ορισμός 2.9.6. Ένας δακτύλιος R θα καλείται περιοχή κυρίων ιδεωδών (Π.Κ.Ι.) εάν:

- (1) Ο R είναι ακέραια περιοχή.
- (2) Κάθε ιδεώδες του R είναι κύριο.

Παράδειγμα 2.9.7. Ο $\mathbb{Z}$ είναι Π.Κ.Ι.

Θεώρημα 2.9.8. Έστω R Π.Κ.Ι. και $I \subseteq R$ ιδεώδες με $I \neq \{0_R\}$. Τότε

$$I \text{ μεγιστικό} \Leftrightarrow I \text{ πρώτο.}$$

Απόδειξη.

($\Rightarrow$) Έστω ότι το I είναι μεγιστικό. Τότε, από το Θεώρημα 2.9.3, το R/I είναι σώμα, άρα ακέραια περιοχή. Επομένως, πάλι από το Θεώρημα 2.9.3, το I είναι πρώτο.

($\Leftarrow$) Έστω ότι το I είναι πρώτο και έστω J ιδεώδες του R με $I \subseteq J$. Επειδή ο R είναι Π.Κ.Ι., υπάρχουν $a, b \in R$ ώστε $I = \langle a \rangle$ και $J = \langle b \rangle$.

Εφόσον $a \in \langle a \rangle = I \subseteq J = \langle b \rangle$, έχουμε $a \in \langle b \rangle$. Άρα υπάρχει $\gamma \in R$ ώστε $a = b\gamma$.

Επειδή $a \in I$, έχουμε $b\gamma \in I$. Εφόσον το I είναι πρώτο, έπεται ότι $b \in I$ ή $\gamma \in I$.

Αν $b \in I$, τότε $\langle b \rangle \subseteq I$, άρα $J \subseteq I$. Επειδή $I \subseteq J$, παίρνουμε $J = I$.

Αν $\gamma \in I = \langle a \rangle$, τότε υπάρχει $c \in R$ ώστε $\gamma = ca$. Επομένως $a = b\gamma = bca$, άρα $a(bc - 1_R) = 0_R$.

Επειδή ο R είναι ακέραια περιοχή, έχουμε $a = 0_R$ ή $bc = 1_R$. Όμως $I \neq \{0_R\}$, άρα $a \neq 0_R$. Επομένως $bc = 1_R$.

Αφού $b \in J$ και το J είναι ιδεώδες, έχουμε $1_R = bc \in J$. Άρα $J = R$.

Συνεπώς το I είναι μεγιστικό.

2.10 Χαρακτηριστική δακτυλίου

Ορισμός 2.10.1.

Έστω R δακτύλιος.

(1) Εάν υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $nr = 0_R$ για κάθε $r \in R$, τότε ορίζουμε ως **χαρακτηριστική** του R τον ελάχιστο θετικό ακέραιο n ώστε $nr = 0_R$ για κάθε $r \in R$.

Η χαρακτηριστική του R συμβολίζεται με $\text{char } R$. Δηλαδή

$$\text{char } R = \min\{n : n \in \mathbb{Z}_{>0} \text{ και } nr = 0_R, \forall r \in R\}.$$

(2) Εάν δεν υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $nr = 0_R$ για κάθε $r \in R$, τότε λέμε ότι ο R έχει **χαρακτηριστική μηδέν**.

Παραδείγματα 2.10.2

(α) Εάν $n \in \mathbb{Z}_{>0}$, τότε

$$\text{char } \mathbb{Z}_n = n.$$

Πράγματι, παρατηρούμε ότι $nr = 0$ για κάθε $r \in \mathbb{Z}_n$ εφόσον, εάν $r = [k]$, τότε $nr = n[k] = [nk] = [0]$.

Επίσης, ο n είναι ο ελάχιστος θετικός ακέραιος ώστε $nr = 0$ για κάθε $r \in \mathbb{Z}_n$.

Πράγματι, έστω ότι υπάρχει $m \in \mathbb{Z}_{>0}$ με $1 \leq m < n$ ώστε $mr = 0$ για κάθε $r \in \mathbb{Z}_n$. Τότε $m[1] = [0]$, δηλαδή $[m] = [0]$, οπότε $n \mid m$, άτοπο.

(β) Ισχύει ότι $\text{char } \mathbb{Z} = 0$, διότι δεν υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $nk = 0$ για κάθε $k \in \mathbb{Z}$.

Ομοίως, $\text{char } \mathbb{R} = 0 = \text{char } \mathbb{Q}$.

Παρατηρήσεις 2.10.3

(1) Έστω R δακτύλιος με μοναδιαίο στοιχείο 1_R .

(α) Εάν $m \in \mathbb{Z}$, $m > 0$, τότε

$$mr = 0_R, \forall r \in R \iff m1_R = 0_R.$$

[Πράγματι το ευθύ είναι προφανές. Για το αντίστροφο, έστω $r \in R$. Τότε

$$mr = m(1_R r) = (m1_R)r = 0_R r = 0_R.]$$

(β) Ισοδύναμος ορισμός της χαρακτηριστικής

Από το (α) προκύπτει ότι ο ορισμός της χαρακτηριστικής θα μπορούσε να δοθεί ως εξής:

- Εάν υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $n1_R = 0_R$, τότε

$$\text{char } R = \text{ο ελάχιστος θετικός ακέραιος } n \text{ ώστε } n1_R = 0_R.$$

- Εάν δεν υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $n1_R = 0_R$, τότε ορίζουμε $\text{char } R = 0$.

(2) Έστω R δακτύλιος με $\text{char } R = n > 0$. Τότε, εάν $k \in \mathbb{Z}_{>0}$, ισχύει

$$kr = 0_R, \forall r \in R \iff n \mid k.$$

Η απόδειξη αφήνεται ως άσκηση (είναι ανάλογη με αυτήν της Πρότασης 2.10.6(3)).

Πρόταση 2.10.4.

Έστω R ακέραια περιοχή. Τότε η χαρακτηριστική του R είναι μηδέν ή πρώτος αριθμός.

Απόδειξη.

Έστω $\text{char } R \neq 0$ και θέτουμε $n = \text{char } R$.

Καταρχάς $n \neq 1$, διότι, εάν $n = 1$, τότε $1_R = 1 \cdot 1_R = 0_R$, άτοπο, αφού ο R είναι ακέραια περιοχή. Άρα $n > 1$.

Έστω προς άτοπο ότι ο n δεν είναι πρώτος.

Τότε υπάρχουν k, ℓ με $1 < k, \ell < n$ ώστε $n = k\ell$.

Έχουμε

$$n1_R = 0_R \iff (k\ell)1_R = 0_R.$$

Επίσης,

$$(k1_R)(\ell 1_R) = \underbrace{(1_R + \cdots + 1_R)}_{k \text{ φορές}} \underbrace{(1_R + \cdots + 1_R)}_{\ell \text{ φορές}} = (k\ell)1_R.$$

Άρα

$$(k1_R)(\ell 1_R) = 0_R.$$

Επειδή ο R είναι ακέραια περιοχή, $k1_R = 0_R$ ή $\ell 1_R = 0_R$.

Αν $k1_R = 0_R$, τότε $\text{char } R \leq k$, άτοπο αφού $k < n$. Ομοίως, δεν μπορεί να ισχύει $\ell 1_R = 0_R$.

Άτοπο. Επομένως ο n είναι πρώτος.

Παρατήρηση 2.10.5.

Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο 1_R και έστω ότι $\text{char } R = p$, όπου p πρώτος. Είναι ο R ακέραια περιοχή;

Απάντηση

Εν γένει όχι. Για παράδειγμα, έστω $R = \mathbb{Z}_3 \times \mathbb{Z}_3$.

Παρατηρούμε ότι

(1) Ο R δεν είναι ακέραια περιοχή, διότι $([1], [0])([0], [1]) = ([0], [0]) = 0_R$ και $([1], [0]), ([0], [1]) \neq ([0], [0])$.

(2) $\text{char } R = 3$.

Πράγματι, παρατηρούμε ότι

$$3([1], [1]) = (3[1], 3[1]) = ([3], [3]) = ([0], [0]) = 0_R.$$

Άρα $\text{char } R \leq 3$.

Έστω ότι υπάρχει $n \in \mathbb{Z}_{>0}$ με $1 \leq n < 3$ ώστε $n([1], [1]) = 0_R$.

Τότε $([n], [n]) = ([0], [0])$, οπότε $[n] = [0]$ στο $\mathbb{Z}_3$.

Άρα $3 \mid n$. Άτοπο.

Πρόταση 2.10.6.

Έστω R δακτύλιος με μοναδιαίο στοιχείο 1_R και $\varphi : \mathbb{Z} \rightarrow R$ με $\varphi(n) = n1_R$, $n \in \mathbb{Z}$.

Τότε

- (1) Η φ είναι ομομορφισμός δακτυλίων.
- (2) $\text{Ker } \varphi \neq \{0\}$ αν και μόνο αν $\text{char } R \neq 0$.
- (3) Εάν $\text{char } R = n$, τότε $\text{Ker } \varphi = \langle n \rangle$.
- (4) Εάν $\text{char } R = n$, τότε $\mathbb{Z}_n \simeq \text{Im } \varphi$.
- (5) Εάν $\text{char } R = 0$, τότε $\mathbb{Z} \simeq \text{Im } \varphi$.

Απόδειξη.

(1) Εύκολο και αφήνεται ως άσκηση.

(2) Έχουμε

$$\text{Ker } \varphi = \{n \in \mathbb{Z} : n1_R = 0_R\}.$$

($\Rightarrow$) Έστω ότι $\text{Ker } \varphi \neq \{0\}$ και έστω $n \in \text{Ker } \varphi$ με $n \neq 0$.

Εάν $n > 0$, τότε $n1_R = 0_R$, άρα $\text{char } R \neq 0$.

Εάν $n < 0$, τότε $n1_R = 0_R$, άρα $(-n)1_R = 0_R$. Εφόσον $-n > 0$, έχουμε και πάλι $\text{char } R \neq 0$.

($\Leftarrow$) Εάν $n = \text{char } R$, τότε $n \in \text{Ker } \varphi$, άρα $\text{Ker } \varphi \neq \{0\}$.

(3) Καταρχάς, εφόσον $n = \text{char } R$, έχουμε $n1_R = 0_R$, άρα $\varphi(n) = 0_R$, δηλαδή $n \in \text{Ker } \varphi$. Επομένως $\langle n \rangle \subseteq \text{Ker } \varphi$.

Αντίστροφα, έστω $m \in \text{Ker } \varphi$. Θα δείξουμε ότι $n \mid m$.

Έστω ότι $m = qn + v$ με $0 \leq v < n$. Θα δείξουμε ότι $v = 0$.

Πράγματι,

$$m1_R = 0_R \Rightarrow (qn + v)1_R = 0_R \Rightarrow (qn)1_R + v1_R = 0_R \Rightarrow q(n1_R) + v1_R = 0_R.$$

Επειδή $n1_R = 0_R$, έχουμε $0_R + v1_R = 0_R$, κι άρα $v1_R = 0_R$.

Άτοπο, διότι ο n είναι ο ελάχιστος θετικός ακέραιος ώστε $n1_R = 0_R$ και $v < n$.

Άρα $v = 0$, επομένως $n \mid m$, δηλαδή $m \in \langle n \rangle$.

Άρα $\text{Ker } \varphi = \langle n \rangle$.

(4) Εφόσον $\text{char } R = n$, από το (3) έχουμε $\text{Ker } \varphi = \langle n \rangle$.

Από το 1ο Θεώρημα Ισομορφισμού Δακτυλίων, $\mathbb{Z} / \text{Ker } \varphi \simeq \text{Im } \varphi$.

Άρα $\mathbb{Z} / \langle n \rangle \simeq \text{Im } \varphi$.

Εφόσον $\mathbb{Z} / \langle n \rangle \simeq \mathbb{Z}_n$, έπεται ότι

$$\mathbb{Z}_n \simeq \text{Im } \varphi.$$

(5) Εφόσον $\text{char } R = 0$, από το (2) έχουμε $\text{Ker } \varphi = \{0\}$.

Άρα η φ είναι 1-1 και, επειδή είναι προφανώς επί στην εικόνα της, αποτελεί ισομορφισμό, δηλαδή η $\varphi : \mathbb{Z} \rightarrow \text{Im } \varphi$ είναι ισομορφισμός. Συνεπώς $\mathbb{Z} \simeq \text{Im } \varphi$.

Πόρισμα 2.10.7.

Έστω R δακτύλιος με μοναδιαίο στοιχείο. Τότε

(1) Εάν $\text{char } R = n$, τότε ο R περιέχει υποδακτύλιο ισόμορφο με τον $\mathbb{Z}_n$.

(2) Εάν $\text{char } R = 0$, τότε ο R περιέχει υποδακτύλιο ισόμορφο με τον $\mathbb{Z}$.