

2.11 Λυμένα Προβλήματα

Άσκηση 1.

Έστω R δακτύλιος ώστε $a^2 = a$ για κάθε $a \in R$.

Ναδειχθεί ότι $2a = 0_R$ για κάθε $a \in R$ και ότι ο R είναι μεταθετικός.

Λύση.

Έστω $a, b \in R$. Τότε

$$(a + b)^2 = a + b \Rightarrow (a + b)(a + b) = a + b$$

$$\Rightarrow a(a + b) + b(a + b) = a + b$$

$$\Rightarrow a^2 + ab + ba + b^2 = a + b$$

$$\Rightarrow a + ab + ba + b = a + b$$

$$\Rightarrow ab + ba = 0. \quad (1)$$

Από (1), για $b = a$, έχουμε

$$a^2 + a^2 = 0_R \Rightarrow a + a = 0_R \Rightarrow 2a = 0_R. \quad (2)$$

Επίσης, από (1),

$$ab = -ba = (-b)a \stackrel{\substack{\text{από (2)} \\ b+b=0_R \\ \text{άρα } -b=b}}{=} ba.$$

Άρα ο R είναι μεταθετικός.

Άσκηση 2.

Έστω R α.π. και έστω ότι υπάρχει $a \in R$ με

$$a \neq 0_R \quad \text{και} \quad 6a = 0_R.$$

Να δειχθεί ότι είτε $2r = 0_R$ για κάθε $r \in R$, είτε $3r = 0_R$ για κάθε $r \in R$.

Λύση.

(Υπενθύμιση) Αν $k \in \mathbb{Z}$, $r \in R$, τότε

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

Έχουμε ότι

$$6a = 0_R \Rightarrow 6(1_R a) = 0_R \stackrel{1_R a + \cdots + 1_R a}{= (1_R + \cdots + 1_R)a} \Rightarrow (6 \cdot 1_R)a = 0_R.$$

Επειδή ο R είναι α.π. και $a \neq 0_R$, έπεται ότι $6 \cdot 1_R = 0_R$.

Τώρα εφόσον $(kr_1)(\ell r_2) = (k\ell)(r_1 r_2)$ για καθε $k, \ell \in \mathbb{Z}$ και καθε $r_1, r_2 \in R$ έχουμε ότι

$$(2 \cdot 1_R)(3 \cdot 1_R) = 0_R.$$

Πάλι εφόσον ο R είναι α.π., έχουμε

$$2 \cdot 1_R = 0_R \quad \text{ή} \quad 3 \cdot 1_R = 0_R.$$

Παρατηρούμε ότι δεν μπορεί να ισχύουν συγχρόνως

$$2 \cdot 1_R = 0_R \quad \text{και} \quad 3 \cdot 1_R = 0_R,$$

διότι τότε

$$3 \cdot 1_R = 0_R \Rightarrow 2 \cdot 1_R + 1_R = 0_R \stackrel{2 \cdot 1_R = 0_R}{\Rightarrow} 1_R = 0_R,$$

άτοπο, αφού ο R είναι α.π. και άρα $1_R \neq 0_R$.

Οπότε είτε $2 \cdot 1_R = 0_R$ είτε $3 \cdot 1_R = 0_R$.

Αν $2 \cdot 1_R = 0_R$, τότε για καθε $r \in R$ έχουμε

$$2r = 2(1_R r) = (2 \cdot 1_R)r = 0_R \cdot r = 0_R.$$

Ομοίως, αν $3 \cdot 1_R = 0_R$, τότε για καθε $r \in R$ έχουμε

$$3r = 3(1_R r) = (3 \cdot 1_R)r = 0_R \cdot r = 0_R.$$

Άσκηση 3.

Έστω R ένας δακτύλιος, $r \in R$.

Το r θα καλείται **μηδενοδύναμο** εάν υπάρχει $\nu \in \mathbb{Z}_{>0}$ ώστε $r^\nu = 0_R$.

Θα συμβολίζουμε με $\text{nil}(R)$ το σύνολο των μηδενοδύναμων στοιχείων του R .

Να βρεθούν τα μηδενοδύναμα του $\mathbb{Z}_{30}$ και $\mathbb{Z}_{60}$.

Λύση.

Έστω $[\alpha] \in \text{nil}(\mathbb{Z}_{30})$. Τότε υπάρχει $\nu \in \mathbb{Z}_{>0}$ ώστε $[\alpha]^\nu = [0]$, δηλαδή

$$\alpha^\nu \equiv 0 \pmod{30}.$$

Άρα

$$\begin{aligned} 30 \mid \alpha^\nu &\Rightarrow 2 \cdot 3 \cdot 5 \mid \alpha^\nu \Rightarrow 2 \mid \alpha^\nu, 3 \mid \alpha^\nu, 5 \mid \alpha^\nu \\ &\Rightarrow 2 \mid \alpha, 3 \mid \alpha, 5 \mid \alpha \xrightarrow[\text{ανά δύο}]{\substack{2,3,5 \\ \text{σχετικά πρώτοι}}} 30 \mid \alpha \Rightarrow [\alpha] = [0]. \end{aligned}$$

Άρα $\text{nil}(\mathbb{Z}_{30}) \subseteq \{[0]\}$. Επειδή προφανώς $[0] \in \text{nil}(\mathbb{Z}_{30})$, έχουμε

$$\text{nil}(\mathbb{Z}_{30}) = \{[0]\}.$$

Ας θεωρήσουμε τώρα το $\text{nil}(\mathbb{Z}_{60})$.

Έστω $[\alpha] \in \text{nil}(\mathbb{Z}_{60})$. Τότε υπάρχει $\nu \in \mathbb{Z}_{>0}$ ώστε $[\alpha]^\nu = [0]$, δηλαδή

$$\alpha^\nu \equiv 0 \pmod{60}.$$

Άρα

$$\begin{aligned} 60 \mid \alpha^\nu &\Rightarrow 2^2 \cdot 3 \cdot 5 \mid \alpha^\nu \Rightarrow 2^2 \mid \alpha^\nu, 3 \mid \alpha^\nu, 5 \mid \alpha^\nu \\ &\Rightarrow 2 \mid \alpha, 3 \mid \alpha, 5 \mid \alpha \xrightarrow[\text{ανά δύο}]{\substack{2,3,5 \\ \text{σχετικά πρώτοι}}} 30 \mid \alpha. \end{aligned}$$

Άρα $\alpha = 0$ ή $\alpha = 30$, δηλαδή $[\alpha] \in \{[0], [30]\}$.

Επομένως $\text{nil}(\mathbb{Z}_{60}) \subseteq \{[0], [30]\}$.

Τώρα

$$30^2 = 30 \cdot 30 = 30 \cdot 2 \cdot 15 = 60 \cdot 15 \equiv 0 \pmod{60} \Rightarrow [30]^2 = [0],$$

Άρα $[30] \in \text{nil}(\mathbb{Z}_{60})$. και επειδή προφανώς $[0] \in \text{nil}(\mathbb{Z}_{60})$, έχουμε τελικά

$$\text{nil}(\mathbb{Z}_{60}) = \{[0], [30]\}.$$

Άσκηση 4.

(1) Να βρεθεί το $\text{nil}(\mathbb{Z}_n)$, όπου $n > 1$.

(2) Ναδειχθεί ότι

$$\text{nil}(\mathbb{Z}_n) = \{[0]\} \Leftrightarrow \text{το } n \text{ δεν διαιρείται με το τετράγωνο πρώτου.}$$

Λύση.

(1) Έστω $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ η ανάλυση του n σε γινόμενο πρώτων, όπου οι $p_1, \dots, p_k$ είναι διαφορετικοί ανά δύο. Θα δείξουμε ότι, για κάθε $m \in \mathbb{Z}$,

$$[m] \in \text{nil}(\mathbb{Z}_n) \Leftrightarrow p_1 p_2 \cdots p_k \mid m.$$

($\Rightarrow$) Έστω $[m] \in \text{nil}(\mathbb{Z}_n)$. Τότε υπάρχει λ θετικός ακέραιος ώστε $[m]^\lambda = [0]$, δηλαδή $n \mid m^\lambda$.

Άρα $p_i \mid m^\lambda$ για κάθε $i = 1, \dots, k$ και, επειδή ο p_i είναι πρώτος, $p_i \mid m$ για κάθε $i = 1, \dots, k$. Επειδή οι $p_1, \dots, p_k$ είναι σχετικά πρώτοι ανά δύο, έπεται ότι $p_1 \cdots p_k \mid m$.

($\Leftarrow$) Έστω $p_1 \cdots p_k \mid m$ και $\lambda = \max\{\nu_1, \dots, \nu_k\}$. Τότε $p_1^\lambda \cdots p_k^\lambda \mid m^\lambda$ και, επειδή $\nu_i \leq \lambda$ για κάθε i , έχουμε $n \mid m^\lambda$. Άρα $[m]^\lambda = [0]$, δηλαδή $[m] \in \text{nil}(\mathbb{Z}_n)$.

Συμπερασματικά

$$\text{nil}(\mathbb{Z}_n) = \{[m] : p_1 \cdots p_k \mid m\} = \langle [p_1 \cdots p_k] \rangle,$$

και το $\text{nil}(\mathbb{Z}_n)$ έχει $\frac{n}{p_1 \cdots p_k}$ στοιχεία, τα $[0], [p_1 \cdots p_k], [2p_1 \cdots p_k], \dots$ (π.χ. $\text{nil}(\mathbb{Z}_{60}) = \langle [30] \rangle = \{[0], [30]\}$, όπως στην Άσκηση 3).

(2) ($\Rightarrow$) Έστω $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ η ανάλυση του n σε γινόμενο πρώτων και έστω ότι κάποιο από τα $\nu_1, \dots, \nu_k$ είναι μεγαλύτερο ή ίσο του 2 (δηλαδή το n διαιρείται από το τετράγωνο πρώτου).

Έστω ότι $\nu_1 \geq 2$. Θέτουμε $m = p_1 \cdots p_k$.

Τότε:

i) $n \nmid m$, διότι εάν $n \mid m$, τότε $p_1^2 \mid m = p_1 \cdots p_k$, άτοπο.

ii) Εάν $\lambda = \max\{\nu_1, \dots, \nu_k\}$, τότε $m^\lambda = p_1^\lambda \cdots p_k^\lambda$ και επειδή $\lambda \geq \nu_i$ για κάθε $i = 1, \dots, k$, έχουμε $n \mid m^\lambda$. Άρα

$$[m]^\lambda = [0].$$

Άρα $[m] \in \text{nil}(\mathbb{Z}_n)$, άτοπο από την υπόθεση εφόσον $[m] \neq [0]$.

Οπότε $\nu_1 = \dots = \nu_k = 1$.

($\Leftarrow$) Αν υποθέσουμε ότι η ανάλυση του n σε γινόμενο πρώτων είναι $n = p_1 p_2 \cdots p_k$ όπου οι $p_1, \dots, p_k$ διαφορετικοί ανά δύο. Έστω επίσης $[m] \in \text{nil}(\mathbb{Z}_n)$. Τότε υπάρχει λ θετικός ακέραιος ώστε $[m]^\lambda = [0]$, άρα $n \mid m^\lambda$, οπότε $p_i \mid m^\lambda$ για κάθε $i = 1, \dots, k$. Επειδή p_i πρώτος, έχουμε $p_i \mid m$ για κάθε $i = 1, \dots, k$. Επειδή οι $p_1, \dots, p_k$ είναι σχετικά πρώτοι ανά δύο, έπεται ότι $p_1 \cdots p_k \mid m$, δηλαδή $n \mid m$. Άρα $[m] = [0]$.

Άσκηση 5.

Αν R μεταθετικός δακτύλιος, τότε το $\text{nil}(R)$ είναι υποδακτύλιος του R .

Λύση.

Καταρχάς $0_R \in \text{nil}(R)$.

Έστω $a, b \in \text{nil}(R)$ και ℓ, κ θετικοί ακέραιοι ώστε $a^\ell = 0_R$, $b^\kappa = 0_R$. Τότε

(i) $ab \in \text{nil}(R)$.

Πράγματι,

$$(ab)^{\kappa\ell} = \underbrace{ab \cdots ab}_{\kappa\ell \text{ φορές}} = (a^\ell)^\kappa (b^\kappa)^\ell = 0_R^\kappa \cdot 0_R^\ell = 0_R,$$

επειδή ο R είναι μεταθετικός. Άρα $ab \in \text{nil}(R)$.

(ii) Για $n = \kappa + \ell$ έχουμε

$$(a+b)^n \stackrel{ab=ba}{=} \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}. \quad (1)$$

Επίσης, για κάθε $i = 0, \dots, n$, έχουμε ότι $i \geq \ell$ ή $n-i \geq \kappa$, διότι εάν $i < \ell$ και $n-i < \kappa$, τότε

$$n = i + n - i < \ell + \kappa = n,$$

άτοπο.

Έστω $i \in \{0, \dots, n\}$.

Εάν $i \geq \ell$, τότε $a^i = a^\ell a^{i-\ell} = 0_R a^{i-\ell} = 0_R$, άρα $a^i b^{n-i} = 0_R$.

Εάν $n-i \geq \kappa$, τότε $b^{n-i} = b^\kappa b^{n-i-\kappa} = 0_R b^{n-i-\kappa} = 0_R$, άρα $a^i b^{n-i} = 0_R$.

Επομένως $a^i b^{n-i} = 0_R$ για κάθε $i = 0, \dots, n$. Άρα, από την (1), $(a+b)^n = 0_R$, οπότε $a+b \in \text{nil}(R)$.

(iii)

$$(-a)^\ell \stackrel{(*)}{=} (-1)^\ell a^\ell = (-1)^\ell 0_R = 0_R,$$

οπότε $-a \in \text{nil}(R)$.

Άρα το $\text{nil}(R)$ είναι υποδακτύλιος του R .

(*) Γνωρίζουμε ότι $(-a)(-b) = ab$, $(-a)b = -ab$ και επίσης $(-a)(-a) = a^2$.

Άρα $(-a)^3 = (-a)(-a)(-a) = a^2(-a) = -a^3$, $(-a)^4 = (-a)^3(-a) = (-a^3)(-a) = a^4$, και συνεχίζοντας επαγωγικά έχουμε ότι

$$(-a)^\ell = \begin{cases} a^\ell, & \text{εάν } \ell \text{ άρτιος,} \\ -a^\ell, & \text{εάν } \ell \text{ περιττός,} \end{cases} = (-1)^\ell a^\ell.$$

Άσκηση 6.

Έστω R δακτύλιος με μοναδιαίο στοιχείο και $r \in R$ μηδενοδύναμο. Ναδειχθεί ότι το $1_R - r$ αντιστρέφεται.

Λύση.

Έστω n θετικός ακέραιος ώστε $r^n = 0_R$. Έχουμε ότι

$$1_R - r^n = (1_R - r)(1_R + r + \cdots + r^{n-1}),$$

αφού $(1_R - r)(1_R + r + \cdots + r^{n-1}) = (1_R + r + \cdots + r^{n-1}) - r - r^2 - \cdots - r^n = 1_R - r^n$.

Οπότε, αφού $r^n = 0_R$, εάν $s = 1_R + r + \cdots + r^{n-1}$, έχουμε ότι $1_R = (1_R - r)s$ και ομοίως $s(1_R - r) = 1_R$. Άρα $1_R - r \in U(R)$.

Άσκηση 7.

Έστω R μεταθετικός με μοναδιαίο στοιχείο, $r \in R$ μηδενοδύναμο και $a \in U(R)$.
Να δειχθεί ότι και τα $a + r$, $a - r$ είναι αντιστρέψιμα.

Λύση.

Έχουμε

$$a + r = a(1_R + a^{-1}r), \quad a - r = a(1_R - a^{-1}r).$$

Επειδή r είναι μηδενοδύναμο, υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $r^n = 0_R$. Άρα $(a^{-1}r)^n = (a^{-1})^n r^n = 0_R$, οπότε το $a^{-1}r$ είναι μηδενοδύναμο.

Από την προηγούμενη άσκηση, τα $1_R + a^{-1}r = 1_R - (-a^{-1}r)$ και $1_R - a^{-1}r$ είναι αντιστρέψιμα. Επομένως και τα $a(1_R + a^{-1}r)$, $a(1_R - a^{-1}r)$ είναι αντιστρέψιμα, δηλαδή $a + r$, $a - r \in U(R)$.

Παρατήρηση

Γιατί δεχόμαστε ότι $\mathbb{Z}_0 = \mathbb{Z}$;

Απάντηση

Παρατηρούμε ότι εάν $a, b \in \mathbb{Z}$, τότε

$$a \equiv b \pmod{0} \iff 0 \mid (a - b) \iff a = b.$$

Άρα, για κάθε $a \in \mathbb{Z}$, $[a]_0 = \{a\}$. Επομένως $\mathbb{Z}_0 = \{\{a\} : a \in \mathbb{Z}\}$, κι άρα μπορούμε να ταυτίσουμε τα $\mathbb{Z}_0$ και $\mathbb{Z}$.

Άσκηση 8.

Έστω $n \in \{0, 1, 2, \dots\}$. Τότε $\mathbb{Z}_n$ α.π. αν και μόνο αν $n = 0$ ή n πρώτος.

Λύση.

($\Rightarrow$) Έστω $\mathbb{Z}_n$ α.π. Έχουμε ότι $n \neq 1$, διότι εάν $n = 1$, τότε $\mathbb{Z}_1 = \{[0]\}$, άρα δεν μπορεί να είναι α.π. (εάν R α.π., τότε $1_R \neq 0_R$, κι άρα ο R μη τετριμμένος.)

Έστω $n > 1$ και έστω ότι ο n δεν είναι πρώτος. Τότε $n = \alpha\beta$, όπου $1 < \alpha, \beta < n$. Άρα $[0] = [n] = [\alpha][\beta]$. Επειδή η $\mathbb{Z}_n$ είναι α.π., έχουμε $[\alpha] = [0]$ ή $[\beta] = [0]$, δηλαδή $n \mid \alpha$ ή $n \mid \beta$, άτοπο, αφού $\alpha, \beta < n$ και $\alpha, \beta > 1$.

($\Leftarrow$) Αν $n = 0$, τότε $\mathbb{Z}_0 = \mathbb{Z}$, άρα είναι α.π.

Έστω τώρα ότι n είναι πρώτος. Τότε ο $\mathbb{Z}_n$ είναι μεταθετικός.

Επίσης $[1] \neq [0]$, αφού αν $[1] = [0]$, τότε $n \mid 1$, άτοπο, επειδή n πρώτος.

Έστω $[\alpha], [\beta] \in \mathbb{Z}_n$ με $[\alpha][\beta] = [0]$. Τότε $n \mid \alpha\beta$. Επειδή ο n είναι πρώτος, έπεται ότι $n \mid \alpha$ ή $n \mid \beta$. Άρα $[\alpha] = [0]$ ή $[\beta] = [0]$.

Επομένως ο $\mathbb{Z}_n$ είναι α.π.

Άσκηση 9.

Έστω R πεπερασμένος δακτύλιος. Δείξτε ότι εάν το $a \in R$ δεν είναι δεξιός μηδενοδιαίρετης, τότε υπάρχει $b \in R$ ώστε $ab = ba = a$.

Λύση.

Εάν $a = 0_R$, τότε προφανώς $ab = ba = a$ για κάθε $b \in R$.

Έστω ότι $a \neq 0_R$ και έστω η $f : R \rightarrow R$ με $f(r) = ra$, $r \in R$.

Η f είναι 1-1.

Πράγματι, έστω $r_1, r_2 \in R$ με $f(r_1) = f(r_2)$.

Τότε $r_1a = r_2a$, άρα $(r_1 - r_2)a = 0_R$ $\xRightarrow{a \text{ όχι δεξιός μηδενοδιαίρετης}}$ $r_1 - r_2 = 0_R$, δηλαδή $r_1 = r_2$.

Επειδή το R είναι πεπερασμένο, η f είναι επί.

Οπότε, εφόσον η f είναι επί και $a \in R$, υπάρχει $b \in R$ ώστε $f(b) = a$, δηλαδή $ba = a$.

Θα δείξουμε ότι και $ab = a$.

Παρατηρούμε ότι

$$(ab - a)a = (ab)a - a^2 = a(ba) - a^2 \stackrel{ba=a}{=} aa - a^2 = 0_R.$$

Άρα $(ab - a)a = 0_R$ $\xRightarrow{a \text{ όχι δεξιός μηδενοδιαίρετης}}$ $ab - a = 0_R$, δηλαδή $ab = a$.

(*) Γενικά, εάν X πεπερασμένο σύνολο και $f : X \rightarrow X$, τότε

$$f \text{ 1-1} \Rightarrow f \text{ επί.}$$

Άσκηση 10.

Έστω R πεπερασμένος δακτύλιος. Αποδείξτε ότι:

- (i) Αν R α.π., τότε R σώμα.
- (ii) Αν R μεταθετικός με μοναδιαίο στοιχείο, τότε κάθε $a \in R \setminus \{0_R\}$ είναι μηδενοδιαιρέτης ή αντιστρέψιμο.
- (iii) Αν R έχει μοναδιαίο στοιχείο, τότε κάθε $a \in R \setminus \{0_R\}$ είναι αντιστρέψιμο ή δεξιός μηδενοδιαιρέτης.

Λύση.

(i) Έστω R α.π. Τότε ο R είναι μεταθετικός με μοναδιαίο στοιχείο. Αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο.

Έστω $a \in R$ με $a \neq 0_R$ και έστω η $f : R \rightarrow R$ με $f(r) = ar$, $r \in R$.

Η f είναι 1-1, διότι εάν $f(r_1) = f(r_2)$, τότε $ar_1 = ar_2$, άρα $a(r_1 - r_2) = 0_R \xrightarrow{R \text{ α.π.}} a = 0_R$ ή $r_1 - r_2 = 0_R$. Επειδή $a \neq 0_R$, έχουμε $r_1 = r_2$.

Εφόσον ο R είναι πεπερασμένος, η f είναι επί. Άρα, επειδή $1_R \in R$, υπάρχει $b \in R$ ώστε $f(b) = 1_R$, δηλαδή $ab = 1_R$. Επειδή ο R είναι μεταθετικός, έχουμε και $ab = ba = 1_R$. Συνεπώς το a είναι αντιστρέψιμο.

(ii) Έστω $a \in R \setminus \{0_R\}$. Εάν το a είναι μηδενοδιαιρέτης, έχουμε το επιθυμητό. Έστω ότι το a δεν είναι μηδενοδιαιρέτης.

Όπως στο (i), η $f : R \rightarrow R$, $f(r) = ar$, είναι 1-1 και άρα επί. Επομένως υπάρχει $b \in R$ ώστε $ab = 1_R$. Επειδή ο R είναι μεταθετικός, $ab = ba = 1_R$, άρα $a \in U(R)$.

(iii) Καταρχάς μία παρατήρηση.

Εάν $a \in R \setminus \{0_R\}$ και υπάρχει $m \in \mathbb{Z}_{>0}$ ώστε $a^m = 1_R$, τότε το a είναι αντιστρέψιμο. Πράγματι, θέτουμε $b = a^{m-1}$. Τότε $a^m = 1_R \Rightarrow aa^{m-1} = a^{m-1}a = 1_R$, άρα $ab = ba = 1_R$.

Ας έλθουμε στην απόδειξη.

Έστω $a \in R \setminus \{0_R\}$. Εάν το a είναι αντιστρέψιμο, έχουμε το επιθυμητό. Έστω ότι το a δεν είναι αντιστρέψιμο.

Θεωρούμε τα στοιχεία $a, a^2, a^3, \dots$. Εφόσον ο R είναι πεπερασμένος, υπάρχουν $m > n > 0$ ώστε $a^m = a^n$.

Πράγματι, εάν $a^m \neq a^n$ για κάθε $m > n$, τότε τα $a, a^2, a^3, \dots$ είναι άπειρα στοιχεία του R διαφορετικά ανά δύο, άτοπο.

Έστω m ο ελάχιστος φυσικός για τον οποίο υπάρχει n φυσικός με $m > n$ και $a^m = a^n$.

Θέτουμε $\beta = a^{m-1} - a^{n-1}$. Τότε $\beta a = (a^{m-1} - a^{n-1})a = a^m - a^n = 0_R$.

Επιπλέον, $\beta \neq 0_R$. Πράγματι, εάν $n > 1$, τότε από $\beta = 0_R$ θα είχαμε $a^{m-1} = a^{n-1}$ με $m-1 > n-1 > 0$, άτοπο από την ελαχιστότητα του m . Εάν $n = 1$, τότε $\beta = a^{m-1} - 1_R$ και από $\beta = 0_R$ θα είχαμε $a^{m-1} = 1_R$, οπότε, από την παραπάνω

παρατήρηση, το a θα ήταν αντιστρέψιμο, άτοπο.
Άρα το a είναι δεξιός μηδενοδιαιρέτης.

Άσκηση 11.

Έστω

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Ναδειχθεί ότι το $\mathbb{Q}(\sqrt{2})$ είναι σώμα με τις συνήθεις πράξεις πραγματικών αριθμών.

Λύση.

Για ευκολία θέτουμε $S = \mathbb{Q}(\sqrt{2})$.

Παρατηρούμε ότι το S είναι υποδακτύλιος του $\mathbb{R}$.

Πράγματι, προφανώς $S \neq \emptyset$ και εάν $s_1 = a_1 + b_1\sqrt{2}$, $s_2 = a_2 + b_2\sqrt{2}$, $s = a + b\sqrt{2} \in S$, τότε

i) $s_1 + s_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in S$, διότι, εφόσον $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, έχουμε $a_1 + a_2, b_1 + b_2 \in \mathbb{Q}$.

ii) $s_1 s_2 = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2} \in S$, διότι $a_1 a_2 + 2b_1 b_2, a_1 b_2 + b_1 a_2 \in \mathbb{Q}$.
και τέλος

iii) $-s = (-a) + (-b)\sqrt{2} \in S$.

Συνεπώς το S είναι υποδακτύλιος του $\mathbb{R}$ και άρα μεταθετικός, εφόσον ο $\mathbb{R}$ είναι μεταθετικός.

Επίσης $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, άρα το $\mathbb{Q}(\sqrt{2})$ έχει μοναδιαίο στοιχείο.

Τέλος, ας δείξουμε ότι κάθε μη μηδενικό στοιχείο του $\mathbb{Q}(\sqrt{2})$ είναι αντιστρέψιμο.

Έστω $s = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ με $s \neq 0$ και ας βρούμε $r = x + y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ώστε $sr = 1$. Έχουμε

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \iff (ax + 2by) + (ay + bx)\sqrt{2} = 1 + 0\sqrt{2},$$

Άρα από (*)

$$\begin{cases} ax + 2by = 1, \\ bx + ay = 0. \end{cases} \quad (\Sigma_1)$$

Η ορίζουσα του (Σ_1) είναι $D = a^2 - 2b^2$.

Παρατηρούμε ότι, επειδή $a \neq 0$ ή $b \neq 0$ (αφού $s \neq 0$), τότε (**) $D \neq 0$.

Οπότε το (Σ_1) έχει μοναδική λύση, την

$$x = \frac{\begin{vmatrix} 1 & 2b \\ 0 & a \end{vmatrix}}{D} = \frac{a}{a^2 - 2b^2} \in \mathbb{Q}, \quad y = \frac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{D} = -\frac{b}{a^2 - 2b^2} \in \mathbb{Q}.$$

Συνεπώς, για

$$r = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2},$$

έχουμε ότι $r \in \mathbb{Q}(\sqrt{2})$ και $sr = rs = 1$.

Άρα το s είναι αντιστρέψιμο και συνεπώς το $\mathbb{Q}(\sqrt{2})$ είναι σώμα.

Παρατηρήσεις

(*) Εάν $a, b, \gamma, \delta \in \mathbb{Q}$ με $a + b\sqrt{2} = \gamma + \delta\sqrt{2}$, τότε $a = \gamma$, $b = \delta$.

Πράγματι, $a + b\sqrt{2} = \gamma + \delta\sqrt{2} \Rightarrow (a - \gamma) + (b - \delta)\sqrt{2} = 0$, οπότε $(b - \delta)\sqrt{2} = \gamma - a$.

Εάν $b \neq \delta$, τότε $\sqrt{2} = \frac{\gamma - a}{b - \delta} \in \mathbb{Q}$, άτοπο. Άρα $b = \delta$ και επομένως $a = \gamma$.

(**) Εάν $a^2 - 2b^2 = 0$, τότε $a^2 = 2b^2$, δηλαδή $|a| = \sqrt{2}|b|$.

Εάν $b \neq 0$, τότε $\sqrt{2} = \frac{|a|}{|b|} \in \mathbb{Q}$, άτοπο. Άρα $b = 0$ και επομένως $a = 0$. Άτοπο αφού $a \neq 0$ ή $b \neq 0$.

Άσκηση 12.

Έστω

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

Ναδειχθεί ότι το S είναι σώμα με τις συνήθεις πράξεις πινάκων.

Λύση.

Πρέπει να δείξουμε ότι:

- (i) Το S είναι δακτύλιος.
- (ii) Το S έχει μοναδιαίο στοιχείο.
- (iii) Το S είναι μεταθετικός.
- (iv) Κάθε $s \in S$ με $s \neq O_S$ είναι αντιστρέψιμο.

Για το (i) έχουμε:

Αρκεί να δείξουμε ότι το S είναι υποδακτύλιος του $M_2(\mathbb{R})$, δηλαδή ότι $s_1 + s_2$, $s_1 s_2$, $-s \in S$ για κάθε $s_1, s_2, s \in S$.

Έστω λοιπόν

$$s_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}, \quad s = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Τότε

$$s_1 + s_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -(b_1 + b_2) & a_1 + a_2 \end{pmatrix} \in S,$$
$$s_1 s_2 = \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + b_1 a_2 \\ -(a_1 b_2 + b_1 a_2) & a_1 a_2 - b_1 b_2 \end{pmatrix} \in S,$$

και

$$-s = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in S.$$

Για το (ii) έχουμε:

Παρατηρούμε ότι

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$$

και

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} I_2 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = I_2 \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

για κάθε $a, b \in \mathbb{R}$.

Άρα το I_2 είναι το μοναδιαίο στοιχείο του S .

Για το (iii) έχουμε:

Εάν

$$s_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in S,$$

τότε εύκολα διαπιστώνουμε ότι $s_1 s_2 = s_2 s_1$.

Για το (iv) έχουμε:

Έστω

$$s = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Θα δείξουμε ότι υπάρχει

$$r = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in S$$

ώστε $sr = I_2$.

Ισοδύναμα,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff \begin{cases} ax - by = 1, \\ bx + ay = 0. \end{cases} \quad (\Sigma_1)$$

Αρκεί να δείξουμε ότι το σύστημα (Σ_1) έχει λύση.

Η ορίζουσα του συστήματος είναι

$$D = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0,$$

εφόσον $a \neq 0$ ή $b \neq 0$.

Άρα το σύστημα έχει μοναδική λύση, την

$$x = \frac{\begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix}}{a^2 + b^2} = \frac{a}{a^2 + b^2},$$

και

$$y = \frac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{a^2 + b^2} = -\frac{b}{a^2 + b^2}.$$

Συνεπώς

$$s^{-1} = \begin{pmatrix} \frac{a}{a^2 + b^2} & -\frac{b}{a^2 + b^2} \\ \frac{b}{a^2 + b^2} & \frac{a}{a^2 + b^2} \end{pmatrix}.$$

Άσκηση 13.

Έστω ο $R = M_2(\mathbb{R})$ εφοδιασμένος με τις συνήθεις πράξεις πινάκων και

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}.$$

Αποδείξτε ότι:

- 1) Ο S υποδακτύλιος του R και επί ο ίδιος δακτύλιος.
- 2) Ο S έχει μοναδιαίο στοιχείο 1_S και μάλιστα $1_S \neq 1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- 3) Ο S είναι ακεραία περιοχή.
- 4) Ο S είναι σώμα.

Λύση.

(1) Καταρχάς προφανώς $S \neq \emptyset$.

Έστω

$$s_1 = \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix}, \quad s = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Τότε

$$s_1 + s_2 = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & 0 \end{pmatrix}, \quad s_1 s_2 = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{pmatrix}, \quad -s = \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix},$$

οπότε $s_1 + s_2, s_1 s_2, -s \in S$.

Άρα ο S είναι υποδακτύλιος του R .

(2) Παρατηρούμε ότι εάν $s = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S$, τότε

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

Οπότε το $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ είναι το μοναδιαίο στοιχείο του S και προφανώς $1_S \neq 1_R$.

(3) Ο S έχει μοναδιαίο στοιχείο $1_S \neq 0_S$.

Επίσης, εάν

$$s_1 = \begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix},$$

τότε

$$s_1 s_2 = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_2 a_1 & 0 \\ 0 & 0 \end{pmatrix} = s_2 s_1,$$

άρα ο S είναι μεταθετικός.

Εάν $s_1 s_2 = 0_S$, τότε

$$\begin{pmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

οπότε $a_1 a_2 = 0$.

Επειδή ο $\mathbb{R}$ είναι α.π., έχουμε $a_1 = 0$ ή $a_2 = 0$, δηλαδή $s_1 = 0_S$ ή $s_2 = 0_S$.

Άρα ο S δεν έχει μηδενοδιαιρέτες και συνεπώς είναι ακεραία περιοχή.

(4) Εφόσον $1_S \neq 0_S$, ο S είναι μεταθετικός. Για να δείξουμε ότι ο S είναι σώμα, αρκεί να δείξουμε ότι κάθε $s \in S$ με $s \neq 0_S$ είναι αντιστρέψιμο.

Έστω $s = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S$ με $s \neq 0_S$, δηλαδή $a \neq 0$.

Τότε, εάν $s' = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}$, έχουμε $ss' = s's = 1_S$. Άρα το s είναι αντιστρέψιμο και

$$s^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

Άσκηση 14.

Έστω

$$S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Ναδειχθεί ότι το S , με τις συνήθεις πράξεις πινάκων,

(i) είναι ακεραία περιοχή,

(ii) δεν είναι σώμα.

Λύση.

(i) Εύκολα δείχνουμε ότι ο S είναι υποδακτύλιος του $M_2(\mathbb{Z})$ και συνεπώς είναι

δακτύλιος με $0_S = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Επίσης ο S είναι μεταθετικός εφόσον εάν

$s_1 = \begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix}$, και $s_2 = \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}$, στοιχεία του S τότε

$$s_1 s_2 = \begin{pmatrix} a_1 a_2 + 2b_1 b_2 & a_1 b_2 + b_1 a_2 \\ 2b_1 a_2 + 2a_1 b_2 & 2b_1 b_2 + a_1 a_2 \end{pmatrix} = s_2 s_1.$$

Επίσης ο S έχει μοναδιαίο στοιχείο το $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Αρκεί να δείξουμε ότι ο S δεν έχει μηδενοδιαϊρέτες.

Έστω

$$s_1 = \begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} \in S$$

με $s_1 s_2 = 0_S$.

Τότε

$$\begin{pmatrix} a_1 a_2 + 2b_1 b_2 & a_1 b_2 + b_1 a_2 \\ 2b_1 a_2 + 2a_1 b_2 & 2b_1 b_2 + a_1 a_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

δηλαδή

$$a_1 a_2 + 2b_1 b_2 = 0, \quad b_1 a_2 + a_1 b_2 = 0.$$

Εάν $s_1 \neq 0_S$, τότε $a_1 \neq 0$ ή $b_1 \neq 0$.

Από τις παραπάνω σχέσεις, το σύστημα

$$a_2 x + 2b_2 y = 0, \quad b_2 x + a_2 y = 0$$

έχει μη μηδενική λύση την $x = a_1, y = b_1$.

Άρα η ορίζουσά του είναι μηδέν, δηλαδή

$$\begin{vmatrix} a_2 & 2b_2 \\ b_2 & a_2 \end{vmatrix} = 0 \Rightarrow a_2^2 - 2b_2^2 = 0.$$

Επειδή $a_2, b_2 \in \mathbb{Z}$, έπεται ότι $a_2 = b_2 = 0$, άρα $s_2 = 0_S$.

Ομοίως, εάν $s_2 \neq 0_S$, τότε $s_1 = 0_S$.

Άρα ο S δεν έχει μηδενοδιαιρέτες και συνεπώς είναι ακεραία περιοχή.

(ii) Θα δείξουμε ότι ο S δεν είναι σώμα.

Έστω $A = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \in S$. Θα δείξουμε ότι ο A δεν είναι αντιστρέψιμος στον S .

Έστω προς άτοπο ότι υπάρχει $B = \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \in S$ ώστε $AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Τότε

$$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

δηλαδή

$$2x + 2y = 1, \quad 2y + x = 0, \quad 2x + 4y = 0, \quad 2y + 2x = 1.$$

Από την πρώτη και την τέταρτη εξίσωση έχουμε

$$2(x + y) = 1,$$

άτοπο, διότι το αριστερό μέλος είναι άρτιος ακέραιος, ενώ το δεξί περιττός.

Άρα ο A δεν είναι αντιστρέψιμος στον S και συνεπώς ο S δεν είναι σώμα.

Άσκηση 15.

Πόσα και ποια είναι τα αντιστρέψιμα στοιχεία

(i) του $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$,

(ii) του $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{35}$.

Λύση.

(i) Από την 2.1.15(3) έχουμε ότι

$$U(\mathbb{Z}_{10} \times \mathbb{Z}_{15}) = U(\mathbb{Z}_{10}) \times U(\mathbb{Z}_{15}).$$

Οπότε

$$\begin{aligned} |U(\mathbb{Z}_{10} \times \mathbb{Z}_{15})| &= |U(\mathbb{Z}_{10})| \cdot |U(\mathbb{Z}_{15})| \\ &= \varphi(10) \cdot \varphi(15) \\ &= \varphi(2 \cdot 5) \cdot \varphi(3 \cdot 5) \\ &= \varphi(2)\varphi(5)\varphi(3)\varphi(5) \\ &= (2-1)(5-1)(3-1)(5-1) = 32 \end{aligned}$$

Επίσης

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

και

$$U(\mathbb{Z}_{15}) = \{[b]_{15} : 1 \leq b \leq 14, (b, 15) = 1\} = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}.$$

Άρα

$$U(\mathbb{Z}_{10} \times \mathbb{Z}_{15}) = U(\mathbb{Z}_{10}) \times U(\mathbb{Z}_{15}) = \{([a]_{10}, [b]_{15}) : a \in \{1, 3, 7, 9\}, b \in \{1, 2, 4, 7, 8, 11, 13, 14\}\}.$$

(ii) Ομοίως, δεδομένου ότι

$$U(\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{35}) = U(\mathbb{Z}_8) \times U(\mathbb{Z}_2) \times U(\mathbb{Z}_{35}).$$

(Γιατί;)

Οπότε

$$|U(\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{35})| = \varphi(8)\varphi(2)\varphi(35) = 4 \cdot 1 \cdot 24 = 96,$$

και

$$U(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}, \quad U(\mathbb{Z}_2) = \{[1]_2\},$$

$$U(\mathbb{Z}_{35}) = \{[c]_{35} : 1 \leq c \leq 34, (c, 35) = 1\} = \{[c]_{35} : 1 \leq c \leq 34, 5 \nmid c, 7 \nmid c\}.$$

Άρα

$$U(\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{35}) = \{([a]_8, [1]_2, [c]_{35}) : a \in \{1, 3, 5, 7\}, 1 \leq c \leq 34, (c, 35) = 1\}.$$

Άσκηση 16.

Έστω

$$A = \begin{pmatrix} 2 & 3 \\ n & m \end{pmatrix} \in M_2(\mathbb{Z}) \quad (n, m \in \mathbb{Z}).$$

Να βρεθούν τα n, m ώστε $A \in U(M_2(\mathbb{Z}))$.

Λύση.

Από το 2.1.12(4) έχουμε ότι

$$\begin{aligned} A \in U(M_2(\mathbb{Z})) &\iff \det A \in U(\mathbb{Z}) = \{1, -1\} \iff \det A = 1 \text{ ή } -1 \\ &\iff 2m - 3n = 1 \text{ ή } 2m - 3n = -1. \end{aligned}$$

Στη συνέχεια για την εύρεση των m, n λύνουμε τις διοφαντικές

$$2m - 3n = 1 \quad \text{και} \quad 2m - 3n = -1.$$

Επειδή $(2, 3) = 1$, εάν (m_0, n_0) είναι μία λύση της $2m - 3n = c$, τότε όλες οι λύσεις της είναι οι $m = m_0 + 3t$, $n = n_0 + 2t$, $t \in \mathbb{Z}$.

Η $2m - 3n = 1$ έχει τη λύση $(m_0, n_0) = (2, 1)$, άρα

$$m = 2 + 3t, \quad n = 1 + 2t, \quad t \in \mathbb{Z}.$$

Η $2m - 3n = -1$ έχει τη λύση $(m_0, n_0) = (1, 1)$, άρα

$$m = 1 + 3t, \quad n = 1 + 2t, \quad t \in \mathbb{Z}.$$

Επομένως $A \in U(M_2(\mathbb{Z}))$ αν και μόνο αν $(m, n) = (2 + 3t, 1 + 2t)$ ή $(m, n) = (1 + 3t, 1 + 2t)$ για κάποιο $t \in \mathbb{Z}$.

Άσκηση 17.

Να βρεθεί το $U(R)$ όταν

(i) $R = \mathbb{Z}[\sqrt{2}]$ (ii) $R = \mathbb{Z}[i]$ (iii) $R = \mathbb{Q}(\sqrt{2})$ (iv) $R = \mathbb{Q}(i)$.

Λύση.

(i) Καταρχάς τα $1, -1 \in U(\mathbb{Z}[\sqrt{2}])$.

Έστω $\tau = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ με $\tau \neq 0$, δηλαδή $m \neq 0$ ή $n \neq 0$.

Τότε

$$\begin{aligned}\tau \in U(\mathbb{Z}[\sqrt{2}]) &\iff \exists k, \lambda \in \mathbb{Z} \text{ ώστε } (m + n\sqrt{2})(k + \lambda\sqrt{2}) = 1 \\ &\iff (mk + 2\lambda n - 1) + (m\lambda + kn)\sqrt{2} = 0.\end{aligned}$$

Επειδή, αν $a, b \in \mathbb{Z}$ και $a + b\sqrt{2} = 0$, τότε $a = b = 0$, έχουμε

$$mk + 2\lambda n = 1 \quad (1)$$

και

$$nk + m\lambda = 0. \quad (2)$$

Διακρίνουμε περιπτώσεις.

α) $n = 0$.

Τότε από την (1) έχουμε $mk = 1$, άρα $m = \pm 1$ και $k = \pm 1$. Επίσης από την (2) έχουμε $m\lambda = 0$. Επειδή $m \neq 0$, έπεται ότι $\lambda = 0$. Άρα $\tau = \pm 1$.

β) $m = 0$.

Τότε από την (1) έχουμε $2\lambda n = 1$, άτοπο.

γ) $m \neq 0$ και $n \neq 0$.

Παρατηρούμε ότι $2n^2 - m^2 \neq 0$, διότι αλλιώς $\sqrt{2} = \frac{|m|}{|n|} \in \mathbb{Q}$, άτοπο. Τότε από τις (1),(2) έχουμε

$$k = \frac{-m}{2n^2 - m^2}, \quad \lambda = \frac{n}{2n^2 - m^2}. \quad (3)$$

Από τις (3) έχουμε $2\lambda^2 - k^2 = \frac{2n^2 - m^2}{(2n^2 - m^2)^2}$, οπότε $(2\lambda^2 - k^2)(2n^2 - m^2) = 1$.

Άρα $2n^2 - m^2 = 1$ ή $2n^2 - m^2 = -1$.

Εάν $2n^2 - m^2 = 1$, τότε $k = -m$, $\lambda = n$, οπότε $\tau^{-1} = -m + n\sqrt{2}$.

Εάν $2n^2 - m^2 = -1$, τότε $k = m$, $\lambda = -n$, οπότε $\tau^{-1} = m - n\sqrt{2}$.

Άρα τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{2}]$ είναι τα $1, -1$ και τα $m + n\sqrt{2}$ για τα οποία $m, n \neq 0$ και $2n^2 - m^2 = 1$ ή $2n^2 - m^2 = -1$.

Για παράδειγμα, τα $1 + \sqrt{2}$, $7 + 5\sqrt{2}$, $3 + 2\sqrt{2}$ είναι αντιστρέψιμα με αντιστρόφους τους $-1 + \sqrt{2}$, $-7 + 5\sqrt{2}$, $3 - 2\sqrt{2}$, αντίστοιχα.

(ii) Καταρχάς τα $1, -1, i, -i \in U(\mathbb{Z}[i])$.

Έστω $\tau = m + ni \in \mathbb{Z}[i]$ με $\tau \neq 0$, δηλαδή $m \neq 0$ ή $n \neq 0$.

Τότε

$$\tau \in U(\mathbb{Z}[i]) \iff \exists k, \lambda \in \mathbb{Z} \text{ ώστε } (m + ni)(k + \lambda i) = 1$$

$$\iff (mk - \lambda n - 1) + (m\lambda + kn)i = 0.$$

Επειδή, αν $a, b \in \mathbb{Z}$ και $a + bi = 0$, τότε $a = b = 0$, έχουμε

$$mk - \lambda n = 1 \quad (4)$$

και

$$m\lambda + kn = 0. \quad (5)$$

Διακρίνουμε περιπτώσεις.

α) $n = 0$.

Τότε από την (4) έχουμε $mk = 1$, άρα $m = \pm 1$ και $k = \pm 1$. Επίσης από την (5) έχουμε $m\lambda = 0$. Επειδή $m \neq 0$, έπεται ότι $\lambda = 0$. Άρα $\tau = \pm 1$.

β) $m = 0$.

Τότε από την (4) έχουμε $-\lambda n = 1$, οπότε $n = \pm 1$ και $\lambda = \mp 1$. Άρα $\tau = \pm i$.

γ) $m \neq 0$ και $n \neq 0$.

Τότε από τις (4),(5) έχουμε

$$k = \frac{m}{m^2 + n^2}, \quad \lambda = \frac{-n}{m^2 + n^2}. \quad (6)$$

Από τις (6) έχουμε $k^2 + \lambda^2 = \frac{m^2 + n^2}{(m^2 + n^2)^2}$, οπότε $(k^2 + \lambda^2)(m^2 + n^2) = 1$.

Άρα $m^2 + n^2 = 1$. Αλλά αυτό είναι αδύνατο, αφού $m, n \neq 0$.

Συνεπώς $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

2ος τρόπος για το (ii).

Θέλουμε το $U(\mathbb{Z}[i])$. Παρατηρούμε ότι $1, -1, i, -i \in U(\mathbb{Z}[i])$.

Πράγματι, γενικά εάν ένας δακτύλιος R έχει 1_R , τότε $1_R, -1_R \in U(R)$. Οπότε, για $R = \mathbb{Z}[i]$, έχουμε $1_R = 1 = 1 + 0i$, άρα $1, -1 \in U(\mathbb{Z}[i])$.

Επίσης $i(-i) = 1$, άρα $i \in U(\mathbb{Z}[i])$ και $i^{-1} = -i$. Ομοίως $(-i)^{-1} = i$.

Έστω τώρα $\tau \in \mathbb{Z}[i]$, $\tau \in U(\mathbb{Z}[i])$ και έστω ότι $\tau = a + bi$. Έχουμε ότι εάν $\tau^{-1} = k + \lambda i$, τότε $1 = \tau\tau^{-1}$, άρα $|1| = |\tau\tau^{-1}|$. Επομένως $1 = |\tau\tau^{-1}| = |\tau||\tau^{-1}|$ και άρα $1 = |\tau|^2|\tau^{-1}|^2$.

Επειδή $\tau = a + bi$ και $\tau^{-1} = k + \lambda i$, έχουμε $|\tau|^2 = a^2 + b^2$ και $|\tau^{-1}|^2 = k^2 + \lambda^2$, που είναι θετικοί ακέραιοι με γινόμενο 1. Άρα $a^2 + b^2 = 1$.

Οπότε, αφού $a, b \in \mathbb{Z}$, έχουμε είτε $a = 0$, $b = \pm 1$, είτε $a = \pm 1$, $b = 0$.

Άρα $\tau = \pm i$ ή $\tau = \pm 1$, δηλαδή $\tau \in \{1, -1, i, -i\}$.

Οπότε $U(\mathbb{Z}[i]) \subseteq \{1, -1, i, -i\}$.

(iii) Επειδή το $\mathbb{Q}(\sqrt{2})$ είναι σώμα, έχουμε $U(\mathbb{Q}(\sqrt{2})) = \mathbb{Q}(\sqrt{2}) \setminus \{0\}$.

(iv) Επειδή το $\mathbb{Q}(i)$ είναι σώμα, έχουμε $U(\mathbb{Q}(i)) = \mathbb{Q}(i) \setminus \{0\}$.

Άσκηση 18.

Έστω R δακτύλιος και S υποδακτύλιος του R .

- (1) Αν ο R έχει μοναδιαίο, δεν ισχύει πάντα ότι έχει και ο S .
- (2) Αν οι R, S έχουν μοναδιαία τα $1_R, 1_S$, δεν ισχύει πάντα ότι $1_R = 1_S$.
- (3) Αν ο R έχει μοναδιαίο το 1_R και $1_R \in S$, τότε ο S έχει μοναδιαίο το 1_R .
- (4) Αν ο R ακέραια περιοχή, $S \neq \{0_R\}$ και ο S έχει μοναδιαίο, τότε $1_S = 1_R$.

Λύση.

(1) Παραδείγματα.

α) $R = \mathbb{Z}, S = 2\mathbb{Z}$.

β) $R = M_2(\mathbb{R})$,

$$S = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Ο S εύκολα φαίνεται ότι είναι υποδακτύλιος του R . Επίσης δεν έχει μοναδιαίο, διότι εάν είχε, έστω $1_S = \begin{pmatrix} 0 & b_0 \\ 0 & 0 \end{pmatrix}$, τότε θα είχαμε

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

Αλλά

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b_0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

(2) Παραδείγματα.

α) $R = \mathbb{Z}_6, S = \{[0], [2], [4]\}$. 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 $1_R = [1] \neq [4] = 1_S$.

β) $R = M_2(\mathbb{R}), S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$. Εύκολα ο S υποδακτύλιος του R . Επίσης το $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ είναι μοναδιαίο του S , εφόσον για κάθε $a \in \mathbb{R}$ έχουμε

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

Οπότε

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

(3) Αφήνεται ως άσκηση.

(4) Έστω $s \in S$ με $s \neq 0_R$. (υπάρχει εφόσον $S \neq \{0_R\}$.)

Επειδή $s \in S$, το 1_S μοναδιαίο του S , έχουμε ότι $s1_S = s$.

Επίσης, επειδή 1_R μοναδιαίο του R , έχουμε $s1_R = s$.

Οπότε $s1_S = s = s1_R$, άρα $s1_S = s1_R$, δηλαδή $s(1_S - 1_R) = 0_R$.

Επειδή ο R είναι α.π., έχουμε $s = 0_R$ ή $1_S - 1_R = 0_R$. Αφού $s \neq 0_R$, έπεται ότι $1_S = 1_R$.

Άσκηση 19.

Έστω R δακτύλιος και S υποδακτύλιος του R . Έστω ότι οι R, S έχουν μοναδιαία $1_R, 1_S$.

(1) Είναι σωστό ότι $U(S) \subseteq U(R)$;

(2) Εάν $1_R = 1_S$, δείξτε ότι $U(S) \subseteq U(R)$.

Λύση.

(1) Εν γένει όχι.

Για παράδειγμα, έστω $R = M_2(\mathbb{R})$, $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$. Έχουμε

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

Παρατηρούμε ότι $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U(S)$, ενώ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin U(R)$.

2ο αντιπαράδειγμα

Έστω $R = \mathbb{Z}_6$ και $S = \{[0], [2], [4]\}$. Εύκολα ο S είναι υποδακτύλιος του R .

Επίσης $1_S = [4]$. Η $[4] \in U(S)$, αλλά $[4] \notin U(R)$, διότι $(4, 6) \neq 1$.

(Το S επίσης είναι σώμα.)

(2) Έστω $s \in U(S)$. Τότε υπάρχει $s' \in S$ ώστε $ss' = s's = 1_S$. Επειδή $1_S = 1_R$, έχουμε $ss' = s's = 1_R$, άρα $s \in U(R)$.

Άσκηση 20.

- (i) Να δειχθεί ότι η $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ με $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$, $a, b \in \mathbb{Q}$, είναι ισομορφισμός.
- (ii) Να δειχθεί ότι η $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ με $\varphi(a + b\sqrt{2}) = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$, δεν είναι ομομορφισμός.
- (iii) Να δειχθεί ότι η $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, $n \geq 2$, με $\varphi(a) = [a]$, $a \in \mathbb{Z}$, είναι επιμορφισμός αλλά όχι 1-1.
- (iv) Η $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}$ με $\varphi([a]) = a$, $[a] \in \mathbb{Z}_n$, είναι ομομορφισμός;
- (v) Εξετάστε εάν η $\varphi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ με $\varphi(n) = 2n$, $n \in \mathbb{Z}$, είναι ομομορφισμός.
- (vi) Η $\varphi : \mathbb{C} \rightarrow \mathbb{R}$ με $\varphi(a + bi) = a$, $a + bi \in \mathbb{C}$, είναι ομομορφισμός;

Λύση.

(i) Η φ είναι καλά ορισμένη, διότι κάθε στοιχείο του $\mathbb{Q}(\sqrt{2})$ γράφεται με μοναδικό τρόπο στη μορφή $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ (Παρατήρηση (*) της Άσκησης 11).

Ας δείξουμε πρώτα ότι η φ είναι ομομορφισμός. Έστω $r_1 = a_1 + b_1\sqrt{2}$, $r_2 = a_2 + b_2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Τότε

$$\begin{aligned}\varphi(r_1 + r_2) &= \varphi((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) \\ &= a_1 + a_2 - (b_1 + b_2)\sqrt{2} \\ &= (a_1 - b_1\sqrt{2}) + (a_2 - b_2\sqrt{2}) \\ &= \varphi(r_1) + \varphi(r_2)\end{aligned}$$

και

$$\begin{aligned}\varphi(r_1 r_2) &= \varphi(a_1 a_2 + 2b_1 b_2 + (a_1 b_2 + a_2 b_1)\sqrt{2}) \\ &= a_1 a_2 + 2b_1 b_2 - (a_1 b_2 + a_2 b_1)\sqrt{2} \\ &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) \\ &= \varphi(r_1)\varphi(r_2).\end{aligned}$$

Επίσης $\text{Ker } \varphi = \{0\}$ και άρα η φ είναι 1-1.

Πράγματι, έστω $r = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Τότε $\varphi(r) = 0 \Leftrightarrow \varphi(a + b\sqrt{2}) = 0 \Leftrightarrow a - b\sqrt{2} = 0 \Leftrightarrow a = b\sqrt{2}$. Εάν $a \neq 0$ ή $b \neq 0$, τότε $a \neq 0$ και $b \neq 0$. Επομένως, επειδή $a = b\sqrt{2}$, έχουμε $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$, άτοπο. Άρα $a = 0$ και $b = 0$, οπότε $r = 0$.

Τέλος, η φ είναι επί. Πράγματι, έστω $w = \gamma + \delta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Τότε για $r = \gamma - \delta\sqrt{2}$ έχουμε $\varphi(r) = \gamma + \delta\sqrt{2} = w$.

(ii) Έστω ότι η φ είναι ομομορφισμός. Τότε, για $r_1 = 1 + \sqrt{2} = r_2$, έχουμε

$$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) \Rightarrow \varphi(3 + 2\sqrt{2}) = (1 + \sqrt{3})(1 + \sqrt{3}) \Rightarrow 3 + 2\sqrt{3} = 4 + 2\sqrt{3},$$

άτοπο.

(iii) Όπως 2.6.2(γ).

- (iv) Η συγκεκριμένη φ δεν είναι καν συνάρτηση, διότι για $a = 0$, $b = n$, έχουμε $[0] = [n]$, αλλά $\varphi([0]) = 0 \neq n = \varphi([n])$.
- (v) Η φ δεν είναι ομομορφισμός, διότι εάν ήταν, για $m_1 = 1$, $m_2 = 1$ θα είχαμε $\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2)$, δηλαδή $\varphi(1) = \varphi(1) \varphi(1)$, άρα $2 = 2 \cdot 2$, άτοπο.
- (vi) Όπως 2.6.2(στ).

Άσκηση 21.

Έστω $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

(i) Ναδειχθεί ότι ο R είναι σώμα με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων.

(ii) Ναδειχθεί ότι η $\varphi : R \rightarrow \mathbb{C}$ με $\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + bi$ είναι ισομορφισμός.

(iii) Από το (ii) να συμπεράνετε ότι υπάρχει $A \in R$ ώστε $A^2 + I = O$.

Λύση.

(i) Έχει γίνει στο 12ο λυμένο.

(ii) Ας δείξουμε πρώτα ότι η φ είναι ομομορφισμός.

Έστω

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad B = \begin{pmatrix} \gamma & \delta \\ -\delta & \gamma \end{pmatrix} \in R.$$

$$\text{Τότε } A + B = \begin{pmatrix} a + \gamma & b + \delta \\ -(b + \delta) & a + \gamma \end{pmatrix} \text{ και } AB = \begin{pmatrix} a\gamma - b\delta & a\delta + b\gamma \\ -(a\delta + b\gamma) & a\gamma - b\delta \end{pmatrix}.$$

Οπότε

$$\varphi(A + B) = (a + \gamma) + (b + \delta)i = (a + bi) + (\gamma + \delta i) = \varphi(A) + \varphi(B),$$

και

$$\begin{aligned} \varphi(AB) &= (a\gamma - b\delta) + (a\delta + b\gamma)i \\ &= (a + bi)(\gamma + \delta i) \\ &= \varphi(A)\varphi(B). \end{aligned}$$

Άρα η φ είναι ομομορφισμός.

Επίσης η φ είναι 1-1, διότι εάν $\varphi(A) = \varphi(B)$, τότε $a + bi = \gamma + \delta i$, άρα $a = \gamma$, $b = \delta$ και επομένως $A = B$.

Η φ είναι επίσης επί.

Πράγματι, έστω $z = a + bi \in \mathbb{C}$. Θέτοντας $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, έχουμε $\varphi(A) = a + bi = z$.

Άρα η φ είναι ισομορφισμός.

(iii) Εφόσον η φ επί, υπάρχει $A \in R$ με $\varphi(A) = i$.

Τότε

$$\varphi(A^2 + I) = \varphi(A^2) + \varphi(I) = (\varphi(A))^2 + 1 = i^2 + 1 = 0.$$

Επειδή η φ είναι 1-1, έχουμε $\text{Ker } \varphi = \{O\}$, άρα

$$\varphi(A^2 + I) = 0 \Rightarrow A^2 + I = O.$$

Άσκηση 22.

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

Λύση.

- (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 μηδενοδιαίρετης του S .

(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

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

Άσκηση 23.

Βρείτε όλους τους ομομορφισμούς $\varphi : R \rightarrow R$ όταν

- (i) $R = \mathbb{Z}$,
- (ii) $R = \mathbb{Q}$.

Λύση.

(i) Δύο ομομορφισμοί από τον $\mathbb{Z}$ στον $\mathbb{Z}$ είναι ο τετριμμένος και ο ταυτοτικός, δηλαδή οι $\varphi_1, \varphi_2 : \mathbb{Z} \rightarrow \mathbb{Z}$ με $\varphi_1(m) = 0$, $\varphi_2(m) = m$ για κάθε $m \in \mathbb{Z}$.

Θα δείξουμε ότι είναι οι μοναδικοί.

Έστω $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ ομομορφισμός μη τετριμμένος. Θα δείξουμε ότι $\varphi = \varphi_2$, δηλαδή $\varphi(m) = m$ για κάθε $m \in \mathbb{Z}$.

Παρατηρούμε ότι $\varphi(1) = 1$. (κοίτα και προηγούμενο πρόβλημα το (5).)

Πράγματι, κατ' αρχάς $\varphi(1) \neq 0$, διότι εάν $\varphi(1) = 0$, τότε για κάθε $m \in \mathbb{Z}$ έχουμε $\varphi(m) = \varphi(m \cdot 1) = \varphi(m)\varphi(1) = 0$, οπότε η φ θα ήταν τετριμμένη, άτοπο.

Τώρα παρατηρούμε ότι

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1),$$

οπότε

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

Άρα $\varphi(1) = 0$ ή $\varphi(1) = 1$. Επειδή $\varphi(1) \neq 0$, έπεται ότι $\varphi(1) = 1$.

Έστω τώρα $m \in \mathbb{Z}$. Έχουμε

$$\varphi(m) = \varphi(m \cdot 1) \stackrel{2.6.3(5)}{=} m \varphi(1) = m \cdot 1 = m.$$

Οπότε $\varphi(m) = m$ για κάθε $m \in \mathbb{Z}$.

(ii) Δύο ομομορφισμοί από τον $\mathbb{Q}$ στον $\mathbb{Q}$ είναι ο τετριμμένος και ο ταυτοτικός, δηλαδή οι $\varphi_1, \varphi_2 : \mathbb{Q} \rightarrow \mathbb{Q}$ με $\varphi_1(r) = 0$, $\varphi_2(r) = r$ για κάθε $r \in \mathbb{Q}$.

Θα δείξουμε ότι είναι οι μοναδικοί.

Έστω $\varphi : \mathbb{Q} \rightarrow \mathbb{Q}$ ομομορφισμός μη τετριμμένος. Θα δείξουμε ότι $\varphi = \varphi_2$.

Όπως στο (i), έχουμε ότι $\varphi(1) = 1$ και από αυτό έπεται

$$\varphi(m) = m \quad \text{για κάθε } m \in \mathbb{Z}. \quad (2)$$

Παρατηρούμε επίσης ότι, εάν n θετικός ακέραιος, τότε

$$1 = \varphi\left(n \cdot \frac{1}{n}\right) = \varphi(n)\varphi\left(\frac{1}{n}\right) \stackrel{(2)}{=} n \varphi\left(\frac{1}{n}\right),$$

και άρα

$$\varphi\left(\frac{1}{n}\right) = \frac{1}{n}. \quad (3)$$

Οπότε, εάν $r \in \mathbb{Q}$ με $r = \frac{m}{n}$, όπου $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, τότε

$$\varphi(r) = \varphi\left(m \cdot \frac{1}{n}\right) = \varphi(m)\varphi\left(\frac{1}{n}\right) \stackrel{(2),(3)}{=} m \cdot \frac{1}{n} = r.$$

Άρα $\varphi(r) = r$ για κάθε $r \in \mathbb{Q}$.

Άσκηση 24.

Βρείτε όλους τους ομομορφισμούς $\varphi : R \rightarrow R$ όταν $R = \mathbb{R}$.

Λύση.

Δύο ομομορφισμοί από τον $\mathbb{R}$ στον $\mathbb{R}$ είναι ο τετριμμένος και ο ταυτοτικός, δηλαδή οι $\varphi_1, \varphi_2 : \mathbb{R} \rightarrow \mathbb{R}$ με $\varphi_1(x) = 0$, $\varphi_2(x) = x$ για κάθε $x \in \mathbb{R}$.

Θα δείξουμε ότι είναι οι μοναδικοί.

Έστω $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ μη τετριμμένος ομομορφισμός. Όπως στο (ii) του προηγούμενου προβλήματος, έχουμε ότι $\varphi(r) = r$ για κάθε $r \in \mathbb{Q}$.

Έστω τώρα $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Θα δείξουμε ότι $\varphi(\alpha) = \alpha$. Θα καταλήξουμε σε άτοπο εάν υποθέσουμε ότι $\varphi(\alpha) \neq \alpha$. Χρειαζόμαστε τον ακόλουθο ισχυρισμό

Ισχυρισμός.

Εάν $x, y \in \mathbb{R}$ με $x > y$, τότε $\varphi(x) > \varphi(y)$.

Απόδειξη ισχυρισμού

Έστω $\theta = x - y > 0$. Θα δείξουμε ότι $\varphi(\theta) > 0$.

Έχουμε ότι $\theta = \sqrt{\theta} \sqrt{\theta}$, οπότε $\varphi(\theta) = \varphi(\sqrt{\theta})\varphi(\sqrt{\theta}) = (\varphi(\sqrt{\theta}))^2 \geq 0$.

Αν $\varphi(\theta) = 0$, τότε για κάθε $z \in \mathbb{R}$ έχουμε $\varphi(z) = \varphi\left(\frac{z}{\theta} \cdot \theta\right) = \varphi\left(\frac{z}{\theta}\right)\varphi(\theta) = 0$, άρα η φ είναι τετριμμένη, άτοπο.

Συνεπώς $\varphi(\theta) > 0$. Άρα $\varphi(x) - \varphi(y) = \varphi(x - y) = \varphi(\theta) > 0$, δηλαδή $\varphi(x) > \varphi(y)$.

Ας δείξουμε τώρα ότι $\varphi(\alpha) = \alpha$.

Έστω ότι $\varphi(\alpha) > \alpha$. Από την πυκνότητα των ρητών, υπάρχει $q \in \mathbb{Q}$ ώστε $\varphi(\alpha) > q > \alpha$. Επειδή $q > \alpha$, από τον ισχυρισμό έχουμε $\varphi(q) > \varphi(\alpha)$. Όμως $\varphi(q) = q$, άρα $q > \varphi(\alpha)$, άτοπο.

Ομοίως καταλήγουμε σε άτοπο εάν υποθέσουμε ότι $\varphi(\alpha) < \alpha$.

Άρα $\varphi(\alpha) = \alpha$ για κάθε $\alpha \in \mathbb{R}$, οπότε η φ είναι η ταυτοτική.

Άσκηση 25.

Βρείτε όλους τους ομομορφισμούς $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$.

Λύση.

Τρεις ομομορφισμοί από τον $\mathbb{Q}(\sqrt{2})$ στον $\mathbb{Q}(\sqrt{2})$ είναι οι $\varphi_1, \varphi_2, \varphi_3 : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ με φ_1 τετριμμένο, φ_2 ταυτοτικό και $\varphi_3(a + b\sqrt{2}) = a - b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$.

Θα δείξουμε ότι είναι οι μοναδικοί.

Έστω $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ μη τετριμμένος ομομορφισμός.

Όπως στα (i),(ii) του προβλήματος 23, έχουμε $\varphi(1) = 1$ και $\varphi(a) = a$ για κάθε $a \in \mathbb{Q}$.

Τώρα παρατηρούμε ότι

$$2 = \varphi(2) = \varphi(\sqrt{2}\sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = (\varphi(\sqrt{2}))^2,$$

οπότε

$$\varphi(\sqrt{2}) = \sqrt{2} \quad \text{ή} \quad \varphi(\sqrt{2}) = -\sqrt{2}.$$

Έστω ότι $\varphi(\sqrt{2}) = \sqrt{2}$. Τότε, για κάθε $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\sqrt{2},$$

δηλαδή $\varphi = \varphi_2$.

Εάν $\varphi(\sqrt{2}) = -\sqrt{2}$, τότε, για κάθε $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b(-\sqrt{2}) = a - b\sqrt{2},$$

οπότε $\varphi = \varphi_3$.

Άσκηση 26.

(i) Βρείτε όλους τους ομομορφισμούς $\varphi : \mathbb{Z} \rightarrow \mathbb{C}$.

(ii) Έστω R α.π. Βρείτε όλους τους ομομορφισμούς $\varphi : \mathbb{Z} \rightarrow R$.

Λύση.

(i) Ένας είναι ο τετριμμένος, δηλαδή $\varphi : \mathbb{Z} \rightarrow \mathbb{C}$ με $\varphi(m) = 0$ για κάθε $m \in \mathbb{Z}$.

Ένας άλλος είναι ο $\varphi : \mathbb{Z} \rightarrow \mathbb{C}$ με $\varphi(m) = m$, $m \in \mathbb{Z}$.

Θα δείξουμε ότι οι δύο παραπάνω είναι οι μοναδικοί.

Έστω $\varphi : \mathbb{Z} \rightarrow \mathbb{C}$ ομομορφισμός μη τετριμμένος. Τότε $\varphi(1) \neq 0$.

Πράγματι, εάν $\varphi(1) = 0$, τότε για κάθε $m \in \mathbb{Z}$ έχουμε

$$\varphi(m) = \varphi(m \cdot 1) \stackrel{2.6.3(5)}{=} m\varphi(1) = 0.$$

Άρα $\varphi(m) = 0$ για κάθε $m \in \mathbb{Z}$, δηλαδή η φ είναι τετριμμένη, άτοπο.

Τώρα παρατηρούμε ότι

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1),$$

οπότε

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

Επειδή ο $\mathbb{C}$ είναι α.π., έχουμε $\varphi(1) = 0$ ή $\varphi(1) = 1$. Αφού $\varphi(1) \neq 0$, έπεται ότι $\varphi(1) = 1$.

Τέλος παρατηρούμε ότι $\varphi(m) = m$ για κάθε $m \in \mathbb{Z}$.

$$\varphi(m) = \varphi(m \cdot 1) \stackrel{2.6.3(5)}{=} m\varphi(1) = m \cdot 1 = m.$$

(ii) Αφήνεται ως άσκηση.

Άσκηση 27.

- (1) Αν $\varphi : R \rightarrow S$ ομομορφισμός, ο R έχει μοναδιαίο το 1_R και $\varphi(1_R) = 0_S$, τότε $\varphi(r) = 0_S$ για κάθε $r \in R$.
- (2) Έστω R δακτύλιος με 1_R και υπάρχει $n \in \mathbb{Z}_{>0}$ ώστε $nr = 0_R$ για κάθε $r \in R$. Αν $\varphi : R \rightarrow \mathbb{Z}$ ομομορφισμός, τότε $\varphi(r) = 0$ για κάθε $r \in R$.
- (3) Ως συνέπεια, αν $n \geq 1$ και $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}$ ομομορφισμός, τότε η φ είναι τετριμμένη.

Λύση.

- (1) Έστω $r \in R$. Τότε

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

- (2) Έχουμε

$$0 = \varphi(0_R) = \varphi(n1_R) \stackrel{2.6.3(5)}{=} \varphi(n \cdot 1_R) = n\varphi(1_R).$$

Επειδή ο $\mathbb{Z}$ είναι α.π. και $n > 0$, έπεται ότι $\varphi(1_R) = 0$. Άρα, από το (1), $\varphi(r) = 0$ για κάθε $r \in R$.

- (3) Στον $\mathbb{Z}_n$ ισχύει $n[a] = [0]$ για κάθε $[a] \in \mathbb{Z}_n$. Άρα, από το (2), κάθε ομομορφισμός $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}$ είναι τετριμμένος.

Άσκηση 28.

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

(1) Υποθέτουμε ότι η φ είναι επί. Ναδειχθεί ότι:

(i) Αν ο R είναι μεταθετικός, τότε και ο S είναι μεταθετικός.

(ii) Αν ο R έχει μοναδιαίο, τότε το $\varphi(1_R)$ είναι μοναδιαίο του S .

(iii) Αν οι R, S έχουν μοναδιαία και $a \in U(R)$, τότε $\varphi(a) \in U(S)$.

(iv) Αν ο R είναι σώμα και ο S μη τετριμμένος, τότε και ο S είναι σώμα.

(2) Αν η φ είναι επί και ο R είναι ακεραία περιοχή, είναι ο S ακεραία περιοχή;

Λύση.

(1) (i) 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

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

(ii) Αρκεί να δείξουμε ότι

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

Έστω $s \in S$. Αφού η φ είναι επί, υπάρχει $r \in R$ με $s = \varphi(r)$.

Άρα

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

και ομοίως $\varphi(1_R) s = s$.

iii) Καταρχάς εφόσον η φ είναι επιμορφισμός, από το (ii) έχουμε ότι το $\varphi(1_R)$ είναι μοναδιαίο του S και από τη μοναδικότητα του μοναδιαίου έχουμε $\varphi(1_R) = 1_S$.

Έστω $a \in U(R)$. Εφόσον $aa^{-1} = 1_R = a^{-1}a$ έχουμε

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

Επειδή $\varphi(1_R) = 1_S$ από την παραπάνω έχουμε

$$\varphi(a) \varphi(a^{-1}) = 1_S = \varphi(a^{-1}) \varphi(a).$$

Άρα

$$\varphi(a) \in U(S) \quad \text{και} \quad (\varphi(a))^{-1} = \varphi(a^{-1}).$$

(iv) Ο S είναι μεταθετικός από το (i). Επίσης από (ii) έχει μοναδιαίο το $\varphi(1_R)$ που είναι διαφορετικό από το μηδενικό του S (γιατί;). Ας δείξουμε τώρα ότι κάθε μη μηδενικό στοιχείο του S είναι αντιστρέψιμο. 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 $r \neq 0_R$. Αφού ο R είναι σώμα, έχουμε $r \in U(R)$. Άρα, από το (iii), $\varphi(r) \in U(S)$, δηλαδή $s \in U(S)$. Επομένως ο S είναι σώμα.

2) Εν γένει δεν ισχύει. Για παράδειγμα, έστω η

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_6, \quad \varphi(m) = [m], \quad m \in \mathbb{Z}.$$

Η φ είναι επιμορφισμός, ο $\mathbb{Z}$ είναι α.π., ενώ ο $\mathbb{Z}_6$ δεν είναι α.π., αφού $[2] \neq [0]$, $[3] \neq [0]$ και $[2][3] = [0]$.

Άσκηση 29.

Έστω $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

- (1) Ναδειχθεί ότι ο R υποδακτύλιος του $M_2(\mathbb{Z})$ και όχι ιδεώδες.
- (2) Η $\varphi : R \rightarrow \mathbb{Z}$ με $\varphi(r) = a + b$ για κάθε $r = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$, είναι ομομορφισμός;
- (3) Υπάρχει $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ επιμορφισμός;
- (4) Ποιο είναι το $U(R)$;

Λύση.

- (1) Καταρχάς $R \neq \emptyset$. Επίσης, εάν $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}, r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \in R$, τότε

$$r_1 + r_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & a_1 + a_2 \end{pmatrix} \in R,$$

$$r_1 r_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 a_2 \\ 0 & a_1 a_2 \end{pmatrix} \in R,$$

και

$$-r_1 = \begin{pmatrix} -a_1 & -b_1 \\ 0 & -a_1 \end{pmatrix} \in R.$$

Άρα R υποδακτύλιος του $M_2(\mathbb{Z})$.

Εάν ο R ήταν ιδεώδες του $M_2(\mathbb{Z})$, τότε για

$$\tau = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z}), \quad r_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R,$$

θα είχαμε ότι $\tau r_1 \in R$, δηλαδή $\tau \in R$, άτοπο.

- (2) Έστω ότι η φ είναι ομομορφισμός.

Τότε για κάθε $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}, r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \in R$ έχουμε

$$\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2)$$

$$\Rightarrow \varphi \left(\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 a_2 \\ 0 & a_1 a_2 \end{pmatrix} \right) = (a_1 + b_1)(a_2 + b_2)$$

$$\Rightarrow a_1 a_2 + a_1 b_2 + b_1 a_2 = a_1 a_2 + a_1 b_2 + b_1 a_2 + b_1 b_2$$

$$\Rightarrow b_1 b_2 = 0 \Rightarrow b_1 = 0 \text{ ή } b_2 = 0,$$

άτοπο.

Άρα η φ δεν είναι ομομορφισμός.

(3) Έστω προς άτοπο ότι υπάρχει $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ επιμορφισμός. Έστω $r = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$. Τότε

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Άρα

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = \varphi\left(a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \varphi\left(b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right).$$

Από το 2.6.3(5) έχουμε

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = a\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + b\varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right). \quad (1)$$

Αφού φ επιμορφισμός, έχουμε $\varphi(1_R) = 1_{\mathbb{Z} \times \mathbb{Z}}$, δηλαδή $\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1, 1)$.

Άρα από την (1) έχουμε

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = (a, a) + b\varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right). \quad (2)$$

Τώρα, εάν $(k, \lambda) = \varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$, έχουμε

$$(k^2, \lambda^2) = \varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) \varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2\right) = \varphi(0_R) = 0_{\mathbb{Z} \times \mathbb{Z}} = (0, 0).$$

Οπότε $k^2 = 0$ και $\lambda^2 = 0$, άρα $k = \lambda = 0$. Επομένως

$$\varphi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = (0, 0). \quad (3)$$

Από τις (2), (3) έπεται ότι, για κάθε $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$, ισχύει $\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = (a, a)$.

Άρα το $(1, 2) \notin \text{Im } \varphi$, οπότε η φ δεν είναι επί. Άτοπο.

(4) Είδαμε στο πρόβλημα 19 ότι εάν R δακτύλιος με μοναδιαίο 1_R και S υποδακτύλιος του R με μοναδιαίο 1_S ώστε $1_R = 1_S$ τότε $U(S) \subseteq U(R)$. Στην προκειμένη περίπτωση ο R υποδακτύλιος του $M_2(\mathbb{Z})$ και έχουν τα ίδια μοναδιαία. Άρα $U(R) \subseteq U(M_2(\mathbb{Z}))$

Έστω $r = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in U(R)$.

Τότε $r \in U(M_2(\mathbb{Z}))$, και άρα $\det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a^2 \in U(\mathbb{Z}) = \{1, -1\}$.

Επομένως $a^2 = 1$, άρα $a = 1$ ή $a = -1$.

Άρα

$$U(R) \subseteq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

Θέτουμε $A_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$ και $A_2 = \left\{ \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} : b \in \mathbb{Z} \right\}$

Θα δείξουμε ότι $A_1 \subseteq U(R)$.

Έστω $r_1 = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in A_1$. Τότε για $r_2 = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$ έχουμε

$$r_1 r_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = r_2 r_1.$$

Άρα $A_1 \subseteq U(R)$.

Έστω $r_1 = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} \in A_2$. Τότε για $r_2 = \begin{pmatrix} -1 & -b \\ 0 & -1 \end{pmatrix}$ έχουμε

$$r_1 r_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = r_2 r_1.$$

Άρα και $A_2 \subseteq U(R)$.

Οπότε

$$U(R) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

Άσκηση 30.

Έστω $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

- (1) Ναδειχθεί ότι ο R υποδακτύλιος του $M_2(\mathbb{Z})$ και να εξετασθεί εάν είναι ιδεώδες.
- (2) Υπάρχει $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ επιμορφισμός;
- (3) Ποιο είναι το $U(R)$;

Λύση.

Αφήνεται ως άσκηση

Άσκηση 31.

Εξετάστε εάν οι δακτύλιοι R, S είναι ισόμορφοι όταν

(1) $R = \mathbb{R}, \quad S = M_2(\mathbb{R})$

(2) $R = \mathbb{Z}, \quad S = \mathbb{Q}$

(3) $R = \mathbb{Z}, \quad S = \mathbb{R}$

(4) $R = \mathbb{Z}, \quad S = 2\mathbb{Z}$

(5) $\mathbb{Q}, \quad \mathbb{Q} \times \mathbb{Q}$

Λύση.

(1) Έστω ότι οι $\mathbb{R}, M_2(\mathbb{R})$ είναι ισόμορφοι. Τότε από το 2.6.16(2), εφόσον ο $\mathbb{R}$ είναι μεταθετικός, έπεται ότι ο S είναι μεταθετικός. Άτοπο.

(2) Έστω ότι οι $\mathbb{Z}, \mathbb{Q}$ ισόμορφοι. Τότε από το 2.6.16(5), εφόσον ο $\mathbb{Q}$ είναι σώμα, έπεται ότι ο $\mathbb{Z}$ σώμα. Άτοπο.

(3) Όμοια με το (2).

(4) Έστω ότι οι $\mathbb{Z}, 2\mathbb{Z}$ ισόμορφοι. Τότε από το 2.6.16(1), εφόσον ο $\mathbb{Z}$ έχει μοναδιαίο στοιχείο, το $2\mathbb{Z}$ έχει μοναδιαίο στοιχείο. Άτοπο.

(5) Έστω ότι οι $\mathbb{Q}, \mathbb{Q} \times \mathbb{Q}$ ισόμορφοι. Τότε από το 2.6.16(4), εφόσον ο $\mathbb{Q}$ είναι α.π., ο $\mathbb{Q} \times \mathbb{Q}$ α.π.

Άτοπο διότι $(1, 0), (0, 1) \in \mathbb{Q} \times \mathbb{Q}, (1, 0), (0, 1) \neq (0, 0)$ και $(1, 0) \cdot (0, 1) = (0, 0)$.

Άσκηση 32.

Δείξτε ότι οι R, S δεν είναι ισόμορφοι όταν

- (1) $R = \mathbb{R}, \quad S = \mathbb{Q}$
- (2) $R = \mathbb{R}, \quad S = \mathbb{C}$
- (3) $R = \mathbb{Q}, \quad S = \mathbb{Q}(i)$
- (4) $R = \mathbb{Q}(\sqrt{2}), \quad S = \mathbb{Q}(\sqrt{3})$

Λύση.

(1) Έστω ότι οι $\mathbb{R}, \mathbb{Q}$ είναι ισόμορφοι και $\varphi : \mathbb{R} \rightarrow \mathbb{Q}$ ισομορφισμός. Έστω $a \in \mathbb{R}$ ώστε $a^2 = 2$. Τότε

$$\varphi(a^2) = \varphi(2) \Rightarrow \varphi(a \cdot a) = \varphi(1 + 1) \Rightarrow \varphi(a)\varphi(a) = \varphi(1) + \varphi(1).$$

Εφόσον φ είναι επιμορφισμός $\varphi(1) = 1$ κι άρα από την παραπάνω έχουμε $(\varphi(a))^2 = 1 + 1 = 2$. Άτοπο, εφόσον $\varphi(a) \in \mathbb{Q}$ και ως γνωστό δεν υπάρχει $q \in \mathbb{Q}$ ώστε $q^2 = 2$.
β' τρόπος

Επειδή η $\varphi : \mathbb{R} \rightarrow \mathbb{Q}$ είναι 1-1 και επί, τα $\mathbb{R}, \mathbb{Q}$ είναι ισοπληθικά. Άτοπο.

(2) Έστω ότι οι $\mathbb{R}, \mathbb{C}$ ισόμορφοι και $\varphi : \mathbb{C} \rightarrow \mathbb{R}$ ισομορφισμός. Έστω $a \in \mathbb{C}$ ώστε $a^2 = -1$. Τότε

$$\varphi(a^2) = \varphi(-1) \xrightarrow{\varphi \text{ ομομ.}} \varphi(a)\varphi(a) = \varphi(-1) \xrightarrow[\text{αφού } \varphi \text{ ομομ.}]{\varphi(-1) = -\varphi(1)} (\varphi(a))^2 = -\varphi(1)$$

$$\xrightarrow[\text{αφού } \varphi \text{ επιμομ.}]{\varphi(1)=1} (\varphi(a))^2 = -1.$$

Άτοπο διότι $\varphi(a) \in \mathbb{R}$ και δεν υπάρχει $x \in \mathbb{R}$ με $x^2 = -1$.

(3) Όμοια με το (2). Αφήνεται ως άσκηση.

(4) Έστω ότι οι $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ ισόμορφοι και $\varphi : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ ισομορφισμός.

Για $a = \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ έχουμε ότι $a^2 = 2$. Άρα

$$\varphi(a^2) = \varphi(2) = \varphi(1+1) \xrightarrow{\varphi \text{ ομομ.}} \varphi(a)\varphi(a) = \varphi(1)+\varphi(1) \xrightarrow[\varphi(1)=1]{\text{αφού } \varphi \text{ επί ομομ.}} (\varphi(a))^2 = 1+1 = 2.$$

Οπότε $\varphi(a) \in \mathbb{Q}(\sqrt{3})$ και $(\varphi(a))^2 = 2$.

Άτοπο διότι δεν υπάρχει $x \in \mathbb{Q}(\sqrt{3})$ ώστε $x^2 = 2$.

Πράγματι, έστω ότι υπάρχει $x = \gamma + \delta\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, όπου $\gamma, \delta \in \mathbb{Q}$ ώστε $x^2 = 2$.

Έχουμε

$$\begin{aligned} x^2 = 2 &\Rightarrow \gamma^2 + 3\delta^2 + 2\gamma\delta\sqrt{3} = 2 \stackrel{(*)}{\Rightarrow} \\ \gamma^2 + 3\delta^2 &= 2 \quad (1) \quad \text{και} \quad 2\gamma\delta = 0 \quad (2) \end{aligned}$$

Από (2) έχουμε $\gamma = 0$ ή $\delta = 0$.

Εάν $\delta = 0$, από (1) έχουμε $\gamma^2 = 2$. Άτοπο εφόσον $\gamma \in \mathbb{Q}$.

Εάν $\gamma = 0$, από (1) έχουμε $\delta^2 = \frac{2}{3}$. Άτοπο, εφόσον $\delta \in \mathbb{Q}$ (**)

(*) Γνωρίζουμε ότι εάν $a, b \in \mathbb{Q}$ και $a + b\sqrt{3} = 0$, τότε $a = b = 0$.

Οπότε εάν $a, b, \gamma, \delta \in \mathbb{Q}$ ώστε $a + b\sqrt{3} = \gamma + \delta\sqrt{3}$, τότε $(a - \gamma) + (b - \delta)\sqrt{3} = 0$

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

(**) Έστω ότι υπάρχει $\delta = \frac{m}{n} \in \mathbb{Q}$ με $\delta^2 = \frac{2}{3}$.

Μπορούμε να υποθέσουμε ότι $(m, n) = 1$.

(Εάν όχι τότε εάν $d = (m, n)$ έχουμε $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$ και $\frac{m/d}{n/d} = \frac{m}{n} = \delta$.

Οπότε για $k = \frac{m}{d}$, $\lambda = \frac{n}{d}$ έχουμε $\delta = \frac{k}{\lambda}$, $(k, \lambda) = 1$.)

Επειδή $\delta^2 = \frac{2}{3}$, έχουμε

$$\frac{m^2}{n^2} = \frac{2}{3} \Rightarrow 3m^2 = 2n^2 \quad (1)$$

Από την (1)

$$2 \mid 3m^2 \stackrel{2 \text{ πρώτος}}{\Rightarrow} 2 \mid m^2 \Rightarrow 2 \mid m \Rightarrow m = 2k.$$

Οπότε από την (1) έχουμε

$$3(2k)^2 = 2n^2 \Rightarrow 12k^2 = 2n^2 \Rightarrow 2(3k^2) = n^2 \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n.$$

Άτοπο εφόσον $(m, n) = 1$.

Άσκηση 33.

Έστω m, n θετικοί ακέραιοι με $m \neq n$. Δείξτε ότι οι $m\mathbb{Z}, n\mathbb{Z}$ δεν είναι ισόμορφοι.

Λύση.

Χωρίς βλάβη της γενικότητας, έστω ότι $m < n$ και ότι οι $m\mathbb{Z}, n\mathbb{Z}$ είναι ισόμορφοι.

Τότε υπάρχει $\varphi : m\mathbb{Z} \rightarrow n\mathbb{Z}$ ισομορφισμός.

Έχουμε ότι $m^2 = m \cdot m$, άρα

$$\varphi(m^2) = \varphi(m)\varphi(m). \quad (1)$$

Επίσης,

$$\varphi(m^2) = \varphi(mm) \xrightarrow[\text{περιπτ. για } k=r=m]{\text{από 2.6.3(5)}} m\varphi(m). \quad (2)$$

Από τις (1), (2) έπεται ότι

$$\varphi(m)\varphi(m) = m\varphi(m) \Rightarrow \varphi(m)\varphi(m) + (-m\varphi(m)) = 0$$

$$\Rightarrow \varphi(m)\varphi(m) - m\varphi(m) = 0 \Rightarrow (\varphi(m) - m)\varphi(m) = 0.$$

Η τελευταία ισότητα ισχύει στον $\mathbb{Z}$ (αφού $\varphi(m) \in n\mathbb{Z} \subseteq \mathbb{Z}$) και, εφόσον ο $\mathbb{Z}$ είναι α.π., έπεται ότι $\varphi(m) = m$ ή $\varphi(m) = 0$.

Αν $\varphi(m) = 0$, τότε $\varphi(z) = 0$ για κάθε $z \in m\mathbb{Z}$.

Πράγματι, εάν $z = mk \in m\mathbb{Z}$, τότε $\varphi(z) = \varphi(mk) = k\varphi(m) = 0$.

Προκύπτει άτοπο, εφόσον η φ είναι ισομορφισμός.

Αν $\varphi(m) = m$, τότε αφού $\varphi(m) \in n\mathbb{Z}$, έπεται ότι $m \in n\mathbb{Z}$, δηλαδή υπάρχει $\lambda \in \mathbb{Z}$ ώστε $m = n\lambda$.

Άτοπο, εφόσον $m < n$.

Παρατήρηση

Έστω R, S ισόμορφοι δακτύλιοι και $\varphi : R \rightarrow S$ ισομορφισμός. Τότε εάν “ p ” μία “αλγεβρική ιδιότητα”, ισχύει ότι

ο R έχει την p ανν ο S έχει την p .

Για παράδειγμα

- (1) R μεταθετικός ανν ο S μεταθετικός.
- (2) Ο R έχει μοναδιαίο ανν ο S έχει μοναδιαίο.
- (3) Ο R είναι α.π. ανν ο S είναι α.π.
- (4) Ο R σώμα ανν ο S είναι σώμα.
- (5) Υπάρχει $r \in R$ με $r \neq 0_R$ ώστε $r^2 = r$ ανν υπάρχει $s \in S$ με $s \neq 0_S$ και $s^2 = s$.
- (6) Υπάρχει $r \in R$ με $r \neq 0_R$ ώστε $2r = 0_R$ ανν υπάρχει $s \in S$ με $s \neq 0_S$ και $2s = 0_S$.
- (7) $3r = 0_R$ για κάθε $r \in R$ ανν $3s = 0_S$ για κάθε $s \in S$.
- (8) Εάν οι R, S έχουν μοναδιαίο, τότε η εξίσωση $x^2 + 1_R = 0_R$ έχει λύση στον R ανν η εξίσωση $x^2 + 1_S = 0_S$ έχει λύση στον S .

κ.ο.κ.

Απόδειξη. των (5)–(8)

Έστω $\varphi : R \rightarrow S$ ισομορφισμός.

- (5) $(\Rightarrow)$ Εφόσον $r^2 = r$, έχουμε

$$\varphi(r^2) = \varphi(r) \xrightarrow{\varphi \text{ ομομ.}} (\varphi(r))^2 = \varphi(r).$$

Άρα για $s = \varphi(r)$ έχουμε $s^2 = s$, και $s \neq 0_S$, αφού $r \neq 0_R$ και η φ είναι 1-1.

- $(\Leftarrow)$ Εφόσον $s^2 = s$, έχουμε $\varphi^{-1}(s^2) = \varphi^{-1}(s)$, άρα

$$(\varphi^{-1}(s))^2 = \varphi^{-1}(s).$$

Οπότε για $r = \varphi^{-1}(s)$ έχουμε το επιθυμητό ($r \neq 0_R$, αφού $s \neq 0_S$).

- (6) Όπως στο (5).

- (7) $(\Rightarrow)$ Έστω $s \in S$. Εφόσον η φ είναι επί, υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Έχουμε

$$3s = s + s + s = \varphi(r) + \varphi(r) + \varphi(r) = \varphi(r + r + r) = \varphi(3r) \stackrel{3r=0_R}{=} \varphi(0_R) = 0_S.$$

- $(\Leftarrow)$ Έστω $r \in R$ και $s = \varphi(r)$. Έχουμε ότι

$$0_S = 3s = 3\varphi(r) = \varphi(3r).$$

Άρα $\varphi(3r) = 0_S$ και επειδή η φ είναι 1-1, έπεται ότι $3r = 0_R$.

(8) $(\Rightarrow)$ Έστω $r \in R$ ώστε $r^2 + 1_R = 0_R$. Τότε

$$\varphi(r^2 + 1_R) = \varphi(0_R) \xrightarrow[\varphi(0_R)=0_S]{\varphi(1_R)=1_S} (\varphi(r))^2 + 1_S = 0_S.$$

Άρα το $s = \varphi(r)$ είναι λύση της εξίσωσης $x^2 + 1_S = 0_S$ στον S .

$(\Leftarrow)$ Έστω $s \in S$ ώστε $s^2 + 1_S = 0_S$ και $r = \varphi^{-1}(s)$. Τότε

$$\begin{aligned} s^2 + 1_S = 0_S &\Rightarrow \varphi^{-1}(s^2 + 1_S) = \varphi^{-1}(0_S) \\ &\Rightarrow (\varphi^{-1}(s))^2 + \varphi^{-1}(1_S) = 0_R \Rightarrow r^2 + 1_R = 0_R. \end{aligned}$$

Άσκηση 34.

Να εξετάσετε εάν οι δακτύλιοι R, S είναι ισόμορφοι όταν

$$(1) \ R = \mathbb{Z}, \ S = \mathbb{R}, \quad (2) \ R = 2\mathbb{Z}, \ S = \mathbb{Z}, \quad (3) \ R = 2\mathbb{Z}, \ S = 3\mathbb{Z},$$

$$(4) \ R = \mathbb{Z}, \ S = M_2(\mathbb{Z}), \quad (5) \ R = \mathbb{Q}, \ S = M_2(\mathbb{Z}), \quad (6) \ R = \mathbb{Z}[\sqrt{2}], \ S = \mathbb{Z}[\sqrt{5}],$$

$$(7) \ R = \mathbb{Z}[i], \ S = \mathbb{Q}(i), \quad (8) \ R = \mathbb{Z}_m, \ S = \mathbb{Z}_n, \ m \neq n.$$

Λύση.

(1) α' τρόπος

Αν $\mathbb{Z}, \mathbb{R}$ ισόμορφοι, τότε εφόσον ο $\mathbb{R}$ σώμα, έπεται ότι ο $\mathbb{Z}$ σώμα. Άτοπο.

β' τρόπος

Αν $\mathbb{Z}, \mathbb{R}$ ισόμορφοι, υπάρχει $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$ ισομορφισμός.

Επειδή η φ είναι 1-1 και επί, τα $\mathbb{Z}, \mathbb{R}$ ισοπληθικά.

Άτοπο.

(2) Εάν οι $2\mathbb{Z}, \mathbb{Z}$ ισόμορφοι, τότε εφόσον ο $\mathbb{Z}$ έχει μοναδιαίο στοιχείο, έπεται ότι ο $2\mathbb{Z}$ έχει μοναδιαίο. Άτοπο (κοίτα 2.1.5(v)).

(3) Έστω ότι οι $2\mathbb{Z}, 3\mathbb{Z}$ ισόμορφοι και έστω $\varphi : 2\mathbb{Z} \rightarrow 3\mathbb{Z}$ ισομορφισμός.

Έχουμε ότι $4 = 2 \cdot 2$, άρα

$$\varphi(4) = \varphi(2)\varphi(2). \quad (1)$$

Επίσης,

$$\varphi(4) = \varphi(2 \cdot 2) = \varphi(2 + 2) = 2\varphi(2). \quad (2)$$

Από τις (1), (2) έχουμε $\varphi(2)\varphi(2) = 2\varphi(2) \Rightarrow \varphi(2)(\varphi(2) - 2) = 0$. Η ισότητα αυτή ισχύει στον $\mathbb{Z}$ (αφού $\varphi(2) \in 3\mathbb{Z} \subseteq \mathbb{Z}$) και, εφόσον ο $\mathbb{Z}$ είναι α.π., έχουμε $\varphi(2) = 0$ ή $\varphi(2) = 2$. Αν $\varphi(2) = 0$, τότε $\varphi(z) = 0$ για κάθε $z \in 2\mathbb{Z}$. Άτοπο αφού η φ είναι 1-1. Αν $\varphi(2) = 2$, τότε $2 \in 3\mathbb{Z}$, άτοπο.

(4) , (5) Αφήνονται ως άσκηση.

(6) Όπως στο 32 (4) από τα λυμένα, δείχνουμε ότι οι $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{5}]$ όχι ισόμορφοι.

(7) Οι R, S όχι ισόμορφοι, διότι ο S σώμα, ενώ ο $\mathbb{Z}[i]$ όχι σώμα, εφόσον εάν ήταν, τότε επειδή $2 \in \mathbb{Z}[i]$ θα υπήρχε $m + ni \in \mathbb{Z}[i]$ ώστε

$$2(m + ni) = 1 \Rightarrow 2m + 2ni = 1 \Rightarrow 2m = 1 \quad \text{και} \quad 2n = 0 \Rightarrow 2m = 1.$$

Άτοπο.

(8) Αν υπάρχει $\varphi : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ ισομορφισμός, τότε, εφόσον η φ είναι 1-1 και επί, τα $\mathbb{Z}_m, \mathbb{Z}_n$ είναι ισοπληθικά. Άρα $m = n$. Άτοπο.

Άσκηση 35.

Να εξετάσετε εάν οι δακτύλιοι R, S είναι ισόμορφοι όταν

$$(1) \quad R = \mathbb{Z}, \quad S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z} \right\}, \quad (2) \quad R = \mathbb{Z}, \quad S = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z} \right\},$$

$$(3) \quad R = \mathbb{Z}[i], \quad S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}, \quad (4) \quad R = \mathbb{Z}[\sqrt{3}], \quad S = \left\{ \begin{pmatrix} a & 3b \\ 3b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\},$$

$$(5) \quad R = \mathbb{Q} \times \mathbb{Q}, \quad S = \mathbb{C}, \quad (6) \quad R = \mathbb{Z}_4, \quad S = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Λύση.

(1) Ναι, είναι ισόμορφοι, εφόσον η $\varphi : \mathbb{Z} \rightarrow S$ με $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $a \in \mathbb{Z}$, είναι ισομορφισμός.

(2) Δεν είναι ισόμορφοι, διότι ο S δεν έχει μοναδιαίο στοιχείο.

Πράγματι, έστω ότι έχει το $1_S = \begin{pmatrix} 0 & b_0 \\ 0 & 0 \end{pmatrix}$. Τότε, επειδή $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in S$, έχουμε

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} 1_S = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b_0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Άτοπο.

β' τρόπος

Ο S δεν είναι α.π., εφόσον εάν $b_1, b_2 \neq 0$, έχουμε

$$\begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(3) Οι R, S είναι ισόμορφοι.

Πράγματι, η $\varphi : R \rightarrow S$ με

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

είναι ισομορφισμός (γιατί;).

(4) Δεν είναι ισόμορφοι.

α' τρόπος

Έστω ότι υπάρχει $\varphi : \mathbb{Z}[\sqrt{3}] \rightarrow S$ ισομορφισμός. Τότε $\varphi(1) = 1_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Έστω $\tau = \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Τότε

$$\varphi(\tau^2) = \varphi(3) = \varphi(1 + 1 + 1) = \varphi(1) + \varphi(1) + \varphi(1) = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}.$$

Επίσης, εάν $\varphi(\tau) = \begin{pmatrix} a & 3b \\ 3b & a \end{pmatrix}$, τότε

$$\varphi(\tau^2) = \varphi(\tau)\varphi(\tau) = \begin{pmatrix} a & 3b \\ 3b & a \end{pmatrix} \begin{pmatrix} a & 3b \\ 3b & a \end{pmatrix} = \begin{pmatrix} a^2 + 9b^2 & 6ab \\ 6ab & a^2 + 9b^2 \end{pmatrix}.$$

Οπότε

$$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \varphi(\tau^2) = \begin{pmatrix} a^2 + 9b^2 & 6ab \\ 6ab & a^2 + 9b^2 \end{pmatrix},$$

άρα $a^2 + 9b^2 = 3$ και $6ab = 0$.

Επομένως $a = 0$ ή $b = 0$.

Εάν $a = 0$, τότε $9b^2 = 3$, άτοπο αφού $b \in \mathbb{Z}$.

Εάν $b = 0$, τότε $a^2 = 3$, άτοπο αφού $a \in \mathbb{Z}$.

β' τρόπος

Ο $\mathbb{Z}[\sqrt{3}]$ είναι α.π., ενώ ο S όχι, εφόσον

$$\begin{pmatrix} 3 & -3 \\ -3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(5) Αφήνεται ως άσκηση.

(6) Έχουμε ότι

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}_2, \bar{0}_2), (\bar{0}_2, \bar{1}_2), (\bar{1}_2, \bar{0}_2), (\bar{1}_2, \bar{1}_2)\}.$$

Παρατηρούμε ότι εάν $r \in \mathbb{Z}_2 \times \mathbb{Z}_2$, τότε

$$2r = r + r = 0_{\mathbb{Z}_2 \times \mathbb{Z}_2} = (\bar{0}_2, \bar{0}_2).$$

Έστω ότι υπάρχει $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_4$ ισομορφισμός.

Έστω $s \in \mathbb{Z}_4$ και $r \in \mathbb{Z}_2 \times \mathbb{Z}_2$ με $\varphi(r) = s$. Έχουμε ότι

$$2s = s + s = \varphi(r) + \varphi(r) = \varphi(r + r) = \varphi(0_{\mathbb{Z}_2 \times \mathbb{Z}_2}) = 0_{\mathbb{Z}_4}.$$

Άρα για κάθε $s \in \mathbb{Z}_4$ έχουμε ότι $2s = 0_{\mathbb{Z}_4}$.

Άτοπο, εφόσον $2\bar{1}_4 = \bar{2}_4 \neq \bar{0}_4$.

Συνεπώς οι $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4$ δεν είναι ισόμορφοι.

Άσκηση 36.

Έστω

$$R = \left\{ \frac{m}{2^a 3^b} : a, b, m \in \mathbb{Z}, a, b \geq 0 \right\}.$$

- (1) Δείξτε ότι ο R είναι δακτύλιος με τις συνήθεις πράξεις και ότι $\mathbb{Z} \subseteq R$.
- (2) Εξετάστε εάν ο R είναι ακέραια περιοχή.
- (3) Είναι ο R ισόμορφος με τον $\mathbb{Q} \times \mathbb{Q}$;
- (4) Δείξτε ότι ο R περιέχεται σε κάθε υποδακτύλιο του $\mathbb{Q}$ που περιέχει τα $\frac{1}{2}, \frac{1}{3}$.
- (5) Δείξτε ότι $\frac{1}{5} \notin R$.
- (6) Είναι ο R σώμα;

Λύση.

- (1) Αρκεί να δείξουμε ότι ο R είναι υποδακτύλιος του $\mathbb{Q}$, δηλαδή ότι $x+y, xy, -x \in R$ για κάθε $x, y \in R$.

Εάν λοιπόν $x = \frac{m}{2^a 3^b}, y = \frac{n}{2^\gamma 3^\delta} \in R$, τότε

$$x + y = \frac{m2^\gamma 3^\delta + n2^a 3^b}{2^{a+\gamma} 3^{b+\delta}} \in R, \quad xy = \frac{mn}{2^{a+\gamma} 3^{b+\delta}} \in R, \quad -x = \frac{-m}{2^a 3^b} \in R.$$

Άρα ο R είναι υποδακτύλιος του $\mathbb{Q}$.

Επίσης, προφανώς εάν $m \in \mathbb{Z}$, τότε $m = \frac{m}{2^0 3^0} \in R$. Άρα $\mathbb{Z} \subseteq R$.

- (2) Μπορούμε να παρατηρήσουμε ότι $1 \in R$, εφόσον $1 = \frac{1}{2^0 3^0} \in R$.

Άρα ο R έχει μοναδιαίο στοιχείο το 1.

Επειδή ο R είναι μεταθετικός δακτύλιος χωρίς μηδενοδιαιρέτες, εφόσον $R \subseteq \mathbb{Q}$ και ο $\mathbb{Q}$ είναι μεταθετικός δακτύλιος χωρίς μηδενοδιαιρέτες, άρα ο R είναι α.π.

- (3) Εάν οι $R, \mathbb{Q} \times \mathbb{Q}$ ήταν ισόμορφοι, τότε, εφόσον ο R είναι α.π., θα έπρεπε και ο $\mathbb{Q} \times \mathbb{Q}$ να είναι α.π.

Όμως παρατηρούμε ότι τα $(1, 0), (0, 1) \neq (0, 0)$ και $(1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0_{\mathbb{Q} \times \mathbb{Q}}$. Άρα ο $\mathbb{Q} \times \mathbb{Q}$ όχι ακέραια περιοχή και συνεπώς δεν είναι ισόμορφος με τον R .

- (4) Εάν S υποδακτύλιος του $\mathbb{Q}$ με $\frac{1}{2}, \frac{1}{3} \in S$, τότε για κάθε $a, b \in \mathbb{Z}$ με $a, b \geq 0$ έχουμε ότι

$$\frac{1}{2^a} = \underbrace{\frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2}}_{a\text{-φορές}} \in S, \quad \frac{1}{3^b} = \underbrace{\frac{1}{3} \cdot \frac{1}{3} \cdots \frac{1}{3}}_{b\text{-φορές}} \in S.$$

Επειδή $1 = \frac{1}{2} + \frac{1}{2} \in S$, έχουμε ότι κάθε $m \in \mathbb{Z}$ ανήκει στο S . Συνεπώς, εάν $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$ με $a, b \geq 0$, τότε $m \in S$, $\frac{1}{2^a 3^b} \in S$, άρα $\frac{m}{2^a 3^b} \in S$.

Συνεπώς κάθε στοιχείο του R είναι και στοιχείο του S . Άρα $R \subseteq S$.

(5) Έστω ότι $\frac{1}{5} \in R$. Τότε υπάρχουν $m, a, b \in \mathbb{Z}$ με $a, b \geq 0$ ώστε

$$\frac{1}{5} = \frac{m}{2^a 3^b} \Rightarrow 5m = 2^a 3^b.$$

Άρα $5 \mid 2^a 3^b$. Άρα $5 \mid 2$ ή $5 \mid 3$. Άτοπο.

(6) Εάν ο R ήταν σώμα, τότε, εφόσον $5 \in R$ και $5 \neq 0$, θα υπήρχε $x \in R$ ώστε

$$5x = 1_R = 1 \Rightarrow x = \frac{1}{5}.$$

Άτοπο, εφόσον $\frac{1}{5} \notin R$.

Άσκηση 37.

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

(1) Αν T είναι υποδακτύλιος του R , ναδειχθεί ότι η $\varphi(T)$ είναι υποδακτύλιος του S .

(2) Αν M είναι υποδακτύλιος του S , ναδειχθεί ότι το $\varphi^{-1}(M)$ είναι υποδακτύλιος του R .

Λύση.

(1) Έχουμε

$$\varphi(T) = \{\varphi(t) : t \in T\}.$$

Εφόσον $0_R \in T$, έχουμε $\varphi(0_R) = 0_S$, άρα $0_S \in \varphi(T)$.

Έστω $s_1, s_2 \in \varphi(T)$. Τότε υπάρχουν $t_1, t_2 \in T$ ώστε $s_1 = \varphi(t_1)$ και $s_2 = \varphi(t_2)$.

Επομένως

$$s_1 + s_2 = \varphi(t_1) + \varphi(t_2) = \varphi(t_1 + t_2) \in \varphi(T),$$

αφού $t_1 + t_2 \in T$.

Επίσης,

$$s_1 s_2 = \varphi(t_1) \varphi(t_2) = \varphi(t_1 t_2) \in \varphi(T),$$

αφού $t_1 t_2 \in T$.

Τέλος,

$$-s_1 = -\varphi(t_1) = \varphi(-t_1) \in \varphi(T),$$

αφού $-t_1 \in T$.

Άρα η $\varphi(T)$ είναι υποδακτύλιος του S .

(2) Έχουμε

$$\varphi^{-1}(M) = \{r \in R : \varphi(r) \in M\}.$$

Εφόσον $0_S \in M$, έχουμε $\varphi(0_R) = 0_S \in M$, άρα $0_R \in \varphi^{-1}(M)$.

Έστω $r_1, r_2 \in \varphi^{-1}(M)$. Τότε $\varphi(r_1), \varphi(r_2) \in M$. Επειδή ο M είναι υποδακτύλιος του S , έχουμε $\varphi(r_1) + \varphi(r_2) \in M$ κι άρα αφού $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ έπεται ότι $\varphi(r_1 + r_2) \in M$ και συνεπώς $r_1 + r_2 \in \varphi^{-1}(M)$.

Όμοια $r_1 r_2 \in \varphi^{-1}(M)$.

Τέλος, $\varphi(-r_1) = -\varphi(r_1) \in M$, οπότε $-r_1 \in \varphi^{-1}(M)$.

Άρα το $\varphi^{-1}(M)$ είναι υποδακτύλιος του R .

Άσκηση 38.

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

(1) Αν I ιδεώδες του R , τότε το $\varphi(I)$ δεν είναι πάντα ιδεώδες του S .

(2) Αν φ επί και I ιδεώδες του R , τότε το $\varphi(I)$ είναι ιδεώδες του S .

(3) Αν J ιδεώδες του S , τότε η $\varphi^{-1}(J)$ είναι ιδεώδες του R .

Λύση.

(1) Θα δώσουμε αντιπαράδειγμα. Έστω $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$ με $\varphi(n) = n$, για κάθε $n \in \mathbb{Z}$. Είναι φανερά η φ ομομορφισμός. Έστω $I = \mathbb{Z}$, το οποίο είναι ιδεώδες του $\mathbb{Z}$. Έχουμε $\varphi(I) = \varphi(\mathbb{Z}) = \{\varphi(n) : n \in \mathbb{Z}\} = \mathbb{Z}$. Το $\mathbb{Z}$ δεν είναι ιδεώδες του $\mathbb{Q}$, διότι αν ήταν, τότε, επειδή $\frac{1}{2} \in \mathbb{Q}$ και $1 \in \mathbb{Z}$, θα είχαμε $\frac{1}{2} \cdot 1 \in \mathbb{Z}$, άτοπο.

(2) Έχουμε $\varphi(I) = \{\varphi(a) : a \in I\}$. Καταρχάς, επειδή I ιδεώδες του R , έχουμε $0_R \in I$, άρα $0_S = \varphi(0_R) \in \varphi(I)$.

Έστω $\beta_1, \beta_2 \in \varphi(I)$. Τότε υπάρχουν $a_1, a_2 \in I$ ώστε $\beta_1 = \varphi(a_1)$ και $\beta_2 = \varphi(a_2)$. Οπότε $\beta_1 - \beta_2 = \varphi(a_1) - \varphi(a_2) = \varphi(a_1 - a_2) \in \varphi(I)$, αφού $a_1 - a_2 \in I$.

Έστω τώρα $s \in S$ και $\beta \in \varphi(I)$. Επειδή $\beta \in \varphi(I)$, υπάρχει $a \in I$ ώστε $\varphi(a) = \beta$. Επειδή η φ είναι επί, υπάρχει $r \in R$ ώστε $s = \varphi(r)$.

Τώρα επειδή I ιδεώδες του R και $a \in I$, έχουμε $ra, ar \in I$.

Επομένως $s\beta = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I)$ και $\beta s = \varphi(a)\varphi(r) = \varphi(ar) \in \varphi(I)$. Άρα το $\varphi(I)$ είναι ιδεώδες του S .

(3) Αφήνεται ως άσκηση.

Άσκηση 39.

(i) Να δείξετε ότι, αν F είναι σώμα, τότε τα μόνα ιδεώδη του F είναι τα $\{0_F\}$ και F .

(ii) Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Να δείξετε ότι, αν τα μόνα ιδεώδη του R είναι τα $\{0_R\}$ και R , τότε ο R είναι σώμα.

Λύση.

(i) Έστω I ιδεώδες του F .

Αν $I = \{0_F\}$, δεν έχουμε τίποτε να δείξουμε.

Έστω λοιπόν $I \neq \{0_F\}$. Τότε υπάρχει $a \in I$ με $a \neq 0_F$.

Επειδή το F είναι σώμα, το στοιχείο a είναι αντιστρέψιμο. Έστω a^{-1} ο αντίστροφος του a .

Εφόσον I είναι ιδεώδες, και $a \in I$, $a^{-1} \in F$ προκύπτει ότι $a^{-1}a = 1_F \in I$.

Τώρα, εάν $b \in F$, τότε επειδή $1_F \in I$ και το I είναι ιδεώδες, παίρνουμε $b = b \cdot 1_F \in I$.

Άρα $F \subseteq I$ και εφόσον προφανώς $I \subseteq F$ έχουμε $I = F$.

Συμπεραίνουμε ότι τα μόνα ιδεώδη του F είναι τα $\{0_F\}$ και F .

(ii) Εφόσον ο R είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, για να δείξουμε ότι ο R είναι σώμα, αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο.

Έστω $a \in R$ με $a \neq 0_R$. Θεωρούμε το κύριο ιδεώδες $\langle a \rangle$.

Επειδή $a \in \langle a \rangle$ (γιατί;) και $a \neq 0_R$, έχουμε $\langle a \rangle \neq \{0_R\}$.

Από την υπόθεση τα μόνα ιδεώδη του R είναι τα $\{0_R\}$ και R . Άρα $\langle a \rangle = R$.

Επομένως $1_R \in \langle a \rangle$ και συνεπώς υπάρχει $r \in R$ ώστε $ra = 1_R$.

Επειδή ο R είναι μεταθετικός, έχουμε επίσης $ar = 1_R$.

Άρα υπάρχει r ώστε $ra = 1_R = ar$, δηλαδή το a είναι αντιστρέψιμο.

Συνεπώς κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο και επομένως ο R είναι σώμα.

Άσκηση 40.

Έστω R δακτύλιος, F σώμα. Εάν $\varphi : F \rightarrow R$ ομομορφισμός, τότε είτε $\varphi \equiv 0$ είτε φ είναι 1-1.

Λύση.

Γνωρίζουμε ότι, εφόσον φ είναι ομομορφισμός, ο $\text{Ker } \varphi$ είναι ιδεώδες του F .

Αφού το F είναι σώμα, από το 2.4.11(α) ή από το (i) του προηγούμενου προβλήματος, έχουμε ότι είτε $\text{Ker } \varphi = \{0_F\}$, οπότε φ είναι 1-1, είτε $\text{Ker } \varphi = F$.

Στην τελευταία περίπτωση $\varphi(a) = 0$ για κάθε $a \in F$.

Δηλαδή $\varphi \equiv 0$.

Άσκηση 41.

(i) Υπάρχει δακτύλιος S και ομομορφισμός δακτυλίων $\varphi : \mathbb{C} \rightarrow S$ τέτοιος ώστε $\text{Ker } \varphi = \mathbb{Q}(i)$;

(ii) Να εξετάσετε αν υπάρχουν $m \geq 2$ και ομομορφισμός δακτυλίων $\varphi : \mathbb{R} \rightarrow \mathbb{Q}$ με $\text{Ker } \varphi = m\mathbb{Z}$.

Λύση.

(i) Όχι.

Πράγματι, επειδή το $\mathbb{C}$ είναι σώμα, από την προηγούμενη άσκηση γνωρίζουμε ότι για κάθε ομομορφισμό δακτυλίων $\varphi : \mathbb{C} \rightarrow S$ ισχύει είτε $\varphi = 0$ είτε η φ είναι 1-1. Στην πρώτη περίπτωση έχουμε $\text{Ker } \varphi = \mathbb{C}$, ενώ στη δεύτερη περίπτωση έχουμε $\text{Ker } \varphi = \{0\}$.

Άρα ο πυρήνας της φ μπορεί να είναι μόνο το $\mathbb{C}$ ή το $\{0\}$.

Επειδή $\mathbb{Q}(i) \neq \{0\}$ και $\mathbb{Q}(i) \neq \mathbb{C}$, δεν υπάρχει τέτοιος ομομορφισμός.

β' τρόπος Επειδή $\text{Ker } \varphi$ είναι ιδεώδες του $\mathbb{C}$, αρκεί να παρατηρήσουμε ότι το $\mathbb{Q}(i)$ δεν είναι ιδεώδες του $\mathbb{C}$. Πράγματι, $1 \in \mathbb{Q}(i)$. Αν το $\mathbb{Q}(i)$ ήταν ιδεώδες του $\mathbb{C}$, τότε για κάθε $z \in \mathbb{C}$ θα είχαμε $z = z \cdot 1 \in \mathbb{Q}(i)$, άρα $\mathbb{C} \subseteq \mathbb{Q}(i)$, άτοπο. Επομένως δεν υπάρχει τέτοιος ομομορφισμός.

(ii) Αφήνεται ως άσκηση

Άσκηση 42.

Έστω F σώμα και $R = M_2(F)$. Δείξτε ότι τα μόνα ιδεώδη του R είναι τα τετριμμένα.

Λύση.

Έστω I ιδεώδες του R . Θα δείξουμε ότι $I = \{0_R\}$ ή $I = R$.

Αρκεί να δείξουμε ότι εάν $I \neq \{0_R\}$, τότε $I = R$.

Έστω λοιπόν $I \neq \{0_R\}$. Τότε υπάρχει $A = \begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix} \in I$ με $A \neq 0_R = \begin{pmatrix} 0_F & 0_F \\ 0_F & 0_F \end{pmatrix}$.

Μπορούμε να υποθέσουμε ότι $a \neq 0_F$. Πράγματι, αφού $A \neq 0_R$, κάποιο στοιχείο a_{ij} του A είναι $\neq 0_F$. Εάν $E_{k\ell}$ είναι ο πίνακας με 1_F στη θέση (k, ℓ) και 0_F στις υπόλοιπες, τότε, επειδή I ιδεώδες,

$$E_{1i}AE_{j1} = a_{ij}E_{11} = \begin{pmatrix} a_{ij} & 0_F \\ 0_F & 0_F \end{pmatrix} \in I,$$

οπότε, αντικαθιστώντας τον A με τον $E_{1i}AE_{j1}$, έχουμε στοιχείο του I με μη μηδενικό το στοιχείο της θέσης $(1, 1)$.

Έστω λοιπόν ότι $a \neq 0_F$. Επειδή I ιδεώδες, $\begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix} \in R$, έχουμε $\begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix} A = \begin{pmatrix} a & b \\ 0_F & 0_F \end{pmatrix} \in I$, οπότε $\begin{pmatrix} a & 0_F \\ 0_F & 0_F \end{pmatrix} = \begin{pmatrix} a & b \\ 0_F & 0_F \end{pmatrix} \begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix} \in I$.

Επειδή το F σώμα, υπάρχει a^{-1} . Άρα $\begin{pmatrix} a^{-1} & 0_F \\ 0_F & 0_F \end{pmatrix} \begin{pmatrix} a & 0_F \\ 0_F & 0_F \end{pmatrix} = \begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix} \in I$.

Ανάλογα, επειδή I ιδεώδες, $\begin{pmatrix} 0_F & 0_F \\ 1_F & 0_F \end{pmatrix} \begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix} \begin{pmatrix} 0_F & 1_F \\ 0_F & 0_F \end{pmatrix} = \begin{pmatrix} 0_F & 0_F \\ 0_F & 1_F \end{pmatrix} \in I$.

Τέλος, επειδή I ιδεώδες, $\begin{pmatrix} 1_F & 0_F \\ 0_F & 0_F \end{pmatrix}, \begin{pmatrix} 0_F & 0_F \\ 0_F & 1_F \end{pmatrix} \in I$, άρα $I_R = \begin{pmatrix} 1_F & 0_F \\ 0_F & 1_F \end{pmatrix} \in I$.

Άρα $I = R$.

Άσκηση 43.

(1) Έστω I ιδεώδες του $\mathbb{Z}$ ώστε $11 \in I$. Αποδείξτε ότι $I = \langle 11 \rangle$ ή $I = \mathbb{Z}$.

(2) Βρείτε όλα τα ιδεώδη I του $\mathbb{Z}$ ώστε $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$.

Λύση.

(1) Έστω I ιδεώδες του $\mathbb{Z}$. Εφόσον ο $\mathbb{Z}$ περιοχή κύριων ιδεωδών (κοίτα 2.4.5), υπάρχει $d \in \mathbb{Z}$ με $d \geq 0$ ώστε $I = \langle d \rangle$.

Εάν $d = 0$, τότε $I = \{0\}$, άτοπο εφόσον $11 \in I$. Άρα $d > 0$.

Επειδή $11 \in I = \langle d \rangle$, έχουμε $d \mid 11$. Άρα $d = 1$ ή $d = 11$.

Επομένως $I = \langle 1 \rangle = \mathbb{Z}$ ή $I = \langle 11 \rangle$.

(2) Έστω I ιδεώδες του $\mathbb{Z}$ με $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$.

Εφόσον ο $\mathbb{Z}$ περιοχή κύριων ιδεωδών, υπάρχει $d \geq 0$ ώστε $I = \langle d \rangle$.

Εάν $d = 0$, τότε $I = \{0\}$, άτοπο αφού $20\mathbb{Z} \subseteq I$. Άρα $d > 0$.

Επειδή $20\mathbb{Z} \subseteq I$, $20 \in 20\mathbb{Z}$ έπεται ότι $20 \in I$ κι άρα $d \mid 20$. Επομένως

$$d = 1 \text{ ή } 2 \text{ ή } 4 \text{ ή } 5 \text{ ή } 10 \text{ ή } 20. \quad (1)$$

Επίσης, επειδή $d \in \langle d \rangle = I \subseteq 2\mathbb{Z}$, έχουμε $d \in 2\mathbb{Z}$, δηλαδή $2 \mid d$. Άρα, από την (1), $d = 2$ ή 4 ή 10 ή 20 .

Επομένως, εάν $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$, τότε $I = \langle 2 \rangle$ ή $I = \langle 4 \rangle$ ή $I = \langle 10 \rangle$ ή $I = \langle 20 \rangle$.

Παρατηρούμε επίσης ότι για $d = 2, 4, 10, 20$ ισχύει $20\mathbb{Z} \subseteq \langle d \rangle \subseteq 2\mathbb{Z}$.

Άρα τα ιδεώδη του $\mathbb{Z}$ που ικανοποιούν $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$ είναι ακριβώς τα $\langle 2 \rangle, \langle 4 \rangle, \langle 10 \rangle, \langle 20 \rangle$.

Άσκηση 44.

(1) Έστω $a, b \in \mathbb{Z} \setminus \{0\}$. Θεωρούμε $I = \{ax + by : x, y \in \mathbb{Z}\}$.

Δείξτε ότι το I είναι ιδεώδες του $\mathbb{Z}$ και ότι $I = \langle d \rangle$, όπου $d = \mu\chi\delta(a, b)$.

(2) Γενικότερα, εάν $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$, $I = \{a_1k_1 + \dots + a_nk_n : k_1, \dots, k_n \in \mathbb{Z}\}$, τότε το I είναι ιδεώδες του $\mathbb{Z}$ και $I = \langle d \rangle$, όπου $d = \mu\chi\delta(a_1, \dots, a_n)$.

Λύση.

(1) Ας δείξουμε ότι το I είναι ιδεώδες του $\mathbb{Z}$.

Προφανώς $I \neq \emptyset$. Επίσης, εάν $e_1 = ax_1 + by_1$, $e_2 = ax_2 + by_2$, όπου $x_i, y_i \in \mathbb{Z}$, $i = 1, 2$, στοιχεία του I , τότε

$$e_1 - e_2 = a(x_1 - x_2) + b(y_1 - y_2) \in I,$$

ενώ, εάν $k \in \mathbb{Z}$, τότε

$$ke_1 = e_1k = a(x_1k) + b(y_1k) \in I.$$

Ας δείξουμε τώρα ότι $I = \langle d \rangle$, όπου $d = \mu\chi\delta(a, b)$.

Καταρχάς $d \in I$, διότι, εφόσον $d = \mu\chi\delta(a, b)$, υπάρχουν $x_0, y_0 \in \mathbb{Z}$ ώστε $d = ax_0 + by_0 \in I$.

Αφού $d \in I$ και I ιδεώδες του $\mathbb{Z}$, έχουμε $kd \in I$ για κάθε $k \in \mathbb{Z}$. Άρα $\langle d \rangle \subseteq I$.

Αντίστροφα, έστω $e = ax + by \in I$. Αφού $d \mid a$ και $d \mid b$, έχουμε $d \mid e$. Άρα $e \in \langle d \rangle$.

Επομένως $I \subseteq \langle d \rangle$ και συνεπώς $I = \langle d \rangle$.

(2) Αφήνεται ως άσκηση.

Άσκηση 45.

(1) Έστω $I = \langle m \rangle$, $J = \langle n \rangle$ ιδεώδη του $\mathbb{Z}$. Δείξτε ότι

$$I + J = \langle d \rangle, \quad d = \mu\chi\delta(m, n), \quad I \cap J = \langle e \rangle, \quad e = \epsilon\chi\pi(m, n), \quad IJ = \langle mn \rangle.$$

(2) Βρείτε $m \in \mathbb{Z}$ ώστε

(i) $\langle m \rangle = \langle 12 \rangle \cap \langle 18 \rangle$.

(ii) $\langle m \rangle = \langle 12 \rangle + \langle 18 \rangle$.

(iii) $\langle m \rangle = \langle 12 \rangle \langle 18 \rangle$.

Λύση.

(1) Η απόδειξη είναι ίδια με την απόδειξη του Παραδείγματος 2.4.10.

Για το πρώτο ζητούμενο δίνουμε και δεύτερο τρόπο. Εφόσον $I = \{mx : x \in \mathbb{Z}\}$ και $J = \{ny : y \in \mathbb{Z}\}$, έχουμε $I + J = \{mx + ny : x, y \in \mathbb{Z}\}$. Άρα, από το προηγούμενο πρόβλημα, παίρνουμε $I + J = \langle d \rangle$, όπου $d = \mu\chi\delta(m, n)$.

(2) Αφήνεται ως άσκηση.

Άσκηση 46.

Έστω R αθέριαια περιουή και $a, b \in R$. Δείξτε ότι

$$\langle a \rangle = \langle b \rangle \iff \text{υπάρχει } u \in U(R) \text{ ώστε } a = ub.$$

Λύση.

($\Rightarrow$) Καταρχάς, εφόσον ο R είναι α.π., έχει μοναδιαίο στοιχείο και άρα $a = 1_R a \in \langle a \rangle$. Οπότε αφού $\langle a \rangle = \langle b \rangle$, άρα $a \in \langle b \rangle$. Επομένως υπάρχει $t \in R$ ώστε $a = tb$.

Ομοίως, $b \in \langle a \rangle$, άρα υπάρχει $s \in R$ ώστε $b = sa$.

Άρα

$$a = tb = tsa \Rightarrow a - tsa = 0_R \Rightarrow (1_R - ts)a = 0_R \xrightarrow{R \text{ α.π.}} a = 0_R \text{ ή } ts = 1_R. \quad (1)$$

Εάν $a = 0_R$, τότε $\langle a \rangle = \{0_R\}$. Άρα $\langle b \rangle = \{0_R\}$ και επομένως $b = 0_R$.

Άρα $a = b = 0_R$. Τότε, για $u = 1_R \in U(R)$, έχουμε $a = ub$.

Εάν $a \neq 0_R$, τότε από την (1) έχουμε $ts = 1_R$. Άρα $t \in U(R)$.

Επομένως για $u = t$ έχουμε $u \in U(R)$ και $a = tb = ub$.

($\Leftarrow$) Ας δείξουμε πρώτα ότι $\langle a \rangle \subseteq \langle b \rangle$.

Έστω $x \in \langle a \rangle$. Τότε υπάρχει $r \in R$ ώστε $x = ra$.

Εφόσον $a = ub$, έχουμε $x = rub = (ru)b$. Άρα $x \in \langle b \rangle$.

Ομοίως, $\langle b \rangle \subseteq \langle a \rangle$, διότι $b = u^{-1}a$. Άρα $\langle a \rangle = \langle b \rangle$.

Άσκηση 47.

(1) Έστω R δακτύλιος, I ιδεώδες του R . Δείξτε ότι εάν υπάρχουν $a, b \in R$ ώστε $a, b \notin I$ και $ab \in I$, τότε ο R/I δεν είναι α.π.

(2) Εξετάστε εάν ο $\mathbb{Z}/I$, $I = \langle 8 \rangle$, είναι α.π.

(3) Εάν I ιδεώδες του $\mathbb{Z}$ με $I = \langle n \rangle$, $n > 1$, δείξτε ότι $\mathbb{Z}/I$ α.π. ανν ο n είναι πρώτος.

Λύση.

(1) Θέτουμε $\omega_1 = a + I$, $\omega_2 = b + I \in R/I$.

Παρατηρούμε ότι $\omega_1, \omega_2 \neq 0_{R/I}$. Πράγματι, εάν $\omega_1 = 0_{R/I}$, τότε $a + I = I$, άρα $a \in I$, άτοπο. Όμοια $\omega_2 \neq 0_{R/I}$.

Επίσης,

$$\omega_1 \omega_2 = (a + I)(b + I) = ab + I \stackrel{ab \in I}{=} I = 0_{R/I}.$$

Άρα τα ω_1, ω_2 είναι μη μηδενικά στοιχεία του R/I με γινόμενο ίσο με $0_{R/I}$. Οπότε ο R/I όχι α.π.

(2) Ο $\mathbb{Z}/I$ δεν είναι α.π., διότι εάν $a = 2$, $b = 4$, τότε $a, b \notin I$, ενώ $ab = 8 \in I$.

Οπότε, δουλεύοντας όπως στο (1), έχουμε ότι ο $\mathbb{Z}/I$ όχι α.π.

(3) $(\Rightarrow)$ Έστω ότι ο n δεν είναι πρώτος και έστω $a, b \in \mathbb{Z}$ ώστε $1 < a, b < n$ και $ab = n$. Τότε $a, b \notin I$, διότι αν $a \in I$, έχουμε $n \mid a$, άτοπο. Ομοίως και $b \notin I$.

Όμως $ab = n \in I$. Οπότε, όπως στο (1), θέτοντας $\omega_1 = a + I$, $\omega_2 = b + I$, έχουμε $\omega_1, \omega_2 \neq 0_{\mathbb{Z}/I}$ και $\omega_1 \omega_2 = I = 0_{\mathbb{Z}/I}$. Άρα το $\mathbb{Z}/I$ δεν είναι α.π.

$(\Leftarrow)$ Καταρχάς, εφόσον ο $\mathbb{Z}$ μεταθετικός με μοναδιαίο στοιχείο, έπεται ότι ο $\mathbb{Z}/I$ μεταθετικός με μοναδιαίο το $1 + I$. Επίσης $1 + I \neq I = 0_{\mathbb{Z}/I}$, αφού $1 \notin \langle n \rangle$ (εφόσον $n > 1$).

Έστω τώρα $a + I, b + I \in \mathbb{Z}/I$ με $(a + I)(b + I) = 0_{\mathbb{Z}/I} = I \Rightarrow ab + I = I$. Άρα $ab \in I$ και εφόσον $I = \langle n \rangle$, έχουμε $n \mid ab$. Συνεπώς επειδή ο n είναι πρώτος, έπεται ότι $n \mid a$ ή $n \mid b$. Άρα $a \in I$ ή $b \in I$.

Επομένως $a + I = I$ ή $b + I = I$, δηλαδή $a + I = 0_{\mathbb{Z}/I}$ ή $b + I = 0_{\mathbb{Z}/I}$.

Οπότε το $\mathbb{Z}/I$ είναι α.π.

Άσκηση 48.

Έστω R δακτύλιος.

- (1) Αν $I = \{0_R\}$, δείξτε ότι $R/I \simeq R$.
- (2) Αν $I = R$, δείξτε ότι $R/I = \{0_{R/I}\}$.

Λύση.

(1) Έχουμε ότι $R/I = \{a + I : a \in R\}$. Αν $a \in R$, τότε $a + I = \{a\}$. Άρα $R/I = \{\{a\} : a \in R\}$.

Έστω η $\varphi : R \rightarrow R$ με $\varphi(a) = a$, $a \in R$. Η φ είναι ισομορφισμός, επομένως είναι 1-1 και άρα $\text{Ker } \varphi = \{0_R\} = I$. Επίσης $\text{Im } \varphi = R$. Από το 1ο Θεώρημα Ισομορφισμών Δακτυλίων (1ο Θ.Ι.Δ.), έχουμε $R/I \simeq \text{Im } \varphi = R$.

Από την απόδειξη του θεωρήματος έχουμε ότι ο ισομορφισμός είναι η $\bar{\varphi} : R/I \rightarrow R$ με $\bar{\varphi}(a + I) = \varphi(a) = a$.

(2) Έστω η $\varphi : R \rightarrow R$ με $\varphi(a) = 0_R$ για κάθε $a \in R$. Τότε $\text{Ker } \varphi = R$ και $\text{Im } \varphi = \{0_R\}$. Άρα, από το 1ο Θεώρημα Ισομορφισμών Δακτυλίων, $R/R \simeq \{0_R\}$.

(Παρατηρούμε ότι $R/R = \{a + R : a \in R\} = \{R\} = \{0_{R/R}\}$.)

Παρατήρηση

Έστω R δακτύλιος, I ιδεώδες του R και S ένας άλλος δακτύλιος.

Εάν θέλουμε να δείξουμε ότι

$$R/I \simeq S,$$

συνήθως αυτό που κάνουμε είναι να βρούμε μια $\varphi : R \rightarrow S$ ώστε

(i) η φ να είναι ομομορφισμός,

(ii) η φ να είναι επί,

(iii) $\text{Ker } \varphi = I$.

Τότε, από το 1ο Θ.Ι.Δ., έχουμε $R/\text{Ker } \varphi \simeq \text{Im } \varphi$ και εφόσον $\text{Ker } \varphi = I$ και $\text{Im } \varphi = S$, έπεται ότι $R/I \simeq S$.

Άσκηση 49.

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 Θ.Ι.Δ., 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

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

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

Άσκηση 50.

Έστω $a, b \in \mathbb{Z}$ με $a \neq 0$, $b \neq 0$ και $I = \{ax + by : x, y \in \mathbb{Z}\}$.

- (1) Δείξτε ότι το I είναι ιδεώδες του $\mathbb{Z}$.
- (2) Δείξτε ότι το I είτε περιέχει όλους τους πρώτους αριθμούς, είτε περιέχει μόνο έναν πρώτο αριθμό, είτε δεν περιέχει κανέναν πρώτο αριθμό.
- (3) Σε ποια από τις τρεις περιπτώσεις του (2) είναι ο $\mathbb{Z}/I$ ακέραια περιοχή;

Λύση.

- (1) Εύκολο.
- (2) Εφόσον το I είναι ιδεώδες του $\mathbb{Z}$, υπάρχει $d \in \mathbb{Z}$, $d > 0$, ώστε $I = \langle d \rangle$.
Επειδή $a = a \cdot 1 + b \cdot 0 \in I$ και $a \neq 0$, έχουμε $I \neq \{0\}$. Άρα $d \neq 0$.
Διακρίνουμε τις περιπτώσεις.
(α) $d = 1$. Τότε $I = \mathbb{Z}$ και περιέχει όλους τους πρώτους αριθμούς.
(β) $d > 1$ και ο d δεν είναι πρώτος. Τότε $I = \{kd : k \in \mathbb{Z}\}$, οπότε το I δεν περιέχει κανέναν πρώτο αριθμό.
(γ) Ο d είναι πρώτος. Τότε το I περιέχει μόνο έναν πρώτο αριθμό, τον d .
- (3) Διακρίνουμε τις παραπάνω περιπτώσεις.
(α) $d = 1$. Τότε $I = \mathbb{Z}$ κι άρα $\mathbb{Z}/\mathbb{Z} = \{a + \mathbb{Z} : a \in \mathbb{Z}\} = \{\mathbb{Z}\} = \{0_{\mathbb{Z}/\mathbb{Z}}\}$.
Συνεπώς ο $\mathbb{Z}/I$ δεν είναι ακέραια περιοχή εφόσον περιέχει μόνο ένα στοιχείο.
(β), (γ) $d > 1$. Από την προηγούμενη άσκηση έχουμε ότι $\mathbb{Z}/I \simeq \mathbb{Z}_d$. Άρα ο $\mathbb{Z}/I$ είναι ακέραια περιοχή ανν ο d είναι πρώτος, δηλαδή μόνο στην περίπτωση (γ).
Επομένως ο $\mathbb{Z}/I$ είναι ακέραια περιοχή μόνο στην περίπτωση που το I περιέχει ακριβώς έναν πρώτο αριθμό.

Άσκηση 51.

Έστω S μεταθετικός δακτύλιος με 1_S και

$$R = \left\{ \begin{pmatrix} \alpha & \beta \\ 0_S & \delta \end{pmatrix} : \alpha, \beta, \delta \in S \right\}.$$

Αποδείξτε ότι

(1) ο R είναι υποδακτύλιος του $M_2(S)$ με $1_R = \begin{pmatrix} 1_S & 0_S \\ 0_S & 1_S \end{pmatrix}$.

(2) Εάν $r = \begin{pmatrix} \alpha & \beta \\ 0_S & \delta \end{pmatrix} \in R$, τότε $r \in U(R)$ ανν $\alpha, \delta \in U(S)$.

(3) Εάν $S = \mathbb{Z}_n$, τότε $|U(R)| = n(\varphi(n))^2$.

Λύση.

(1) Το R περιέχει τον μηδενικό πίνακα. Επίσης, εάν $A_1, A_2 \in R$, με

$$A_1 = \begin{pmatrix} a_1 & \beta_1 \\ 0 & \delta_1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} a_2 & \beta_2 \\ 0 & \delta_2 \end{pmatrix},$$

τότε

$$A_1 + A_2 = \begin{pmatrix} a_1 + a_2 & \beta_1 + \beta_2 \\ 0 & \delta_1 + \delta_2 \end{pmatrix} \in R, \quad A_1 A_2 = \begin{pmatrix} a_1 a_2 & a_1 \beta_2 + \beta_1 \delta_2 \\ 0 & \delta_1 \delta_2 \end{pmatrix} \in R$$

και

$$-A_1 = \begin{pmatrix} -a_1 & -\beta_1 \\ 0 & -\delta_1 \end{pmatrix} \in R.$$

Άρα ο R είναι υποδακτύλιος του $M_2(S)$.

(2) $(\Rightarrow)$ Έστω $r = \begin{pmatrix} \alpha & \beta \\ 0_S & \delta \end{pmatrix} \in U(R)$ και $r^{-1} = \begin{pmatrix} \gamma & \lambda \\ 0_S & \mu \end{pmatrix}$.

Έχουμε $rr^{-1} = 1_R$, δηλαδή

$$\begin{pmatrix} \alpha\gamma & \alpha\lambda + \beta\mu \\ 0_S & \delta\mu \end{pmatrix} = \begin{pmatrix} 1_S & 0_S \\ 0_S & 1_S \end{pmatrix}.$$

Άρα $\alpha\gamma = 1_S$ και $\delta\mu = 1_S$. Επειδή ο S είναι μεταθετικός, $\gamma\alpha = 1_S$ και $\mu\delta = 1_S$.

Άρα $\alpha, \delta \in U(S)$.

$(\Leftarrow)$ Έστω ότι $\alpha, \delta \in U(S)$. Θέτουμε

$$r' = \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}\beta\delta^{-1} \\ 0_S & \delta^{-1} \end{pmatrix}.$$

Έχουμε $rr' = 1_R$ και $r'r = 1_R$. Άρα $r \in U(R)$ και $r^{-1} = r'$.

(3) Από το (2) έχουμε ότι

$$U(R) = \left\{ \begin{pmatrix} [\alpha] & [\beta] \\ [0] & [\delta] \end{pmatrix} : [\alpha], [\delta] \in U(\mathbb{Z}_n), [\beta] \in \mathbb{Z}_n \right\}.$$

Υπάρχουν $\varphi(n)$ επιλογές για το $[\alpha]$, $\varphi(n)$ επιλογές για το $[\delta]$ και n επιλογές για το $[\beta]$. Επομένως $|U(R)| = \varphi(n) \cdot \varphi(n) \cdot n = n(\varphi(n))^2$.

Άσκηση 52.

Έστω p πρώτος και $R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}_p \right\}$.

Αποδείξτε ότι

- (1) ο R είναι υποδακτύλιος του $M_2(\mathbb{Z}_p)$, αλλά όχι ιδεώδες του $M_2(\mathbb{Z}_p)$.
- (2) Το σύνολο $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in \mathbb{Z}_p \right\}$ είναι ιδεώδες του R και ότι $R/I \simeq \mathbb{Z}_p$.
- (3) Πόσα στοιχεία του R είναι αντιστρέψιμα;

Λύση.

(1) Εύκολα ο R είναι υποδακτύλιος του $M_2(\mathbb{Z}_p)$.

Θα δείξουμε ότι ο R δεν είναι ιδεώδες του $M_2(\mathbb{Z}_p)$.

Πράγματι, εάν ήταν ιδεώδες, τότε για

$$s = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z}_p), \quad r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in R,$$

θα έπρεπε να ισχύει $sr \in R$.

Όμως $sr = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \notin R$. Άρα ο R δεν είναι ιδεώδες του $M_2(\mathbb{Z}_p)$.

(2) Ας δείξουμε πρώτα ότι το I είναι ιδεώδες του R .

Καταρχάς, προφανώς $I \neq \emptyset$.

Έστω $s_1 = \begin{pmatrix} 0 & b_1 \\ 0 & d_1 \end{pmatrix}, s_2 = \begin{pmatrix} 0 & b_2 \\ 0 & d_2 \end{pmatrix} \in I$ και $r = \begin{pmatrix} \kappa & \lambda \\ 0 & \mu \end{pmatrix} \in R$.

Τότε $s_1 - s_2 = \begin{pmatrix} 0 & b_1 - b_2 \\ 0 & d_1 - d_2 \end{pmatrix} \in I, rs_1 = \begin{pmatrix} 0 & \kappa b_1 + \lambda d_1 \\ 0 & \mu d_1 \end{pmatrix} \in I$ και $s_1 r = \begin{pmatrix} 0 & b_1 \mu \\ 0 & d_1 \mu \end{pmatrix} \in I$.

Άρα το I είναι ιδεώδες του R .

Θα δείξουμε τώρα ότι $R/I \simeq \mathbb{Z}_p$.

Θεωρούμε την απεικόνιση $\varphi : R \rightarrow \mathbb{Z}_p$ με $\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = a$.

Έχουμε ότι:

1) Η φ είναι ομομορφισμός.

Πράγματι, εάν $r_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \in R, i = 1, 2$, τότε

$$\varphi(r_1 + r_2) = a_1 + a_2 = \varphi(r_1) + \varphi(r_2) \text{ και } \varphi(r_1 r_2) = a_1 a_2 = \varphi(r_1) \varphi(r_2).$$

2) $\text{Ker } \varphi = I$.

Πράγματι, εάν $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$ τότε

$$r \in \text{Ker } \varphi \iff \varphi(r) = 0 \iff a = 0 \iff r \in I.$$

3) Η φ είναι επί.

Πράγματι, εάν $a \in \mathbb{Z}_p$, τότε για $r = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in R$ έχουμε $\varphi(r) = a$.

Τώρα από το 1ο Θ.Ι.Δ., έχουμε ότι $R/\text{Ker } \varphi \simeq \text{Im } \varphi$ και εφόσον $\text{Ker } \varphi = I$ και $\text{Im } \varphi = \mathbb{Z}_p$, έπεται ότι $R/I \simeq \mathbb{Z}_p$.

(3) Από την προηγούμενη άσκηση γνωρίζουμε ότι, εάν

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}_n \right\},$$

τότε

$$|U(S)| = n(\varphi(n))^2.$$

Στη συγκεκριμένη άσκηση $n = p$. Επομένως

$$|U(R)| = p(\varphi(p))^2 = p(p-1)^2.$$

Παρατήρηση

Η βασική ιδέα είναι να βρούμε έναν ομομορφισμό $\varphi : R \rightarrow \mathbb{Z}_p$ ώστε $\text{Ker } \varphi = I$ και $\text{Im } \varphi = \mathbb{Z}_p$.

Για να βρούμε μια τέτοια φ , δουλεύουμε ως εξής.

Προσπαθούμε να δούμε τι είναι αυτό που διακρίνει δύο στοιχεία του R/I .

Στην περίπτωσή μας, εάν $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in R$, τότε

$$r_1 + I = r_2 + I \iff r_1 - r_2 \in I \iff \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & d_1 - d_2 \end{pmatrix} \in I \iff a_1 - a_2 = 0 \iff a_1 = a_2.$$

Συνεπώς

$$r_1 + I \neq r_2 + I \iff a_1 \neq a_2.$$

Οπότε, εάν $r + I \in R/I$, όπου $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, αυτό που διακρίνει το $r + I$ από τα υπόλοιπα στοιχεία του R/I είναι η τιμή που παίρνει το a .

Θεωρούμε λοιπόν την απεικόνιση $\varphi : R \rightarrow \mathbb{Z}_p$ με $\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = a$.

Άσκηση 53.

Έστω $R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$, δηλαδή R είναι το σύνολο των άνω τριγωνικών πινάκων του $M_2(\mathbb{Z})$, και $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\}$.

- (1) Δείξτε ότι ο R είναι υποδακτύλιος του $M_2(\mathbb{Z})$.
- (2) Δείξτε ότι το I είναι ιδεώδες του R και ότι R/I ισόμορφος με τον $\mathbb{Z} \times \mathbb{Z}$.
- (3) Είναι το I πρώτο ιδεώδες του R ;

Λύση.

- (1) Αφήνεται ως άσκηση.

(2) Καταρχάς $I \neq \emptyset$. Επίσης, εάν $s_1 = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix}$, $s_2 = \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix} \in I$ και $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$, τότε $s_1 - s_2 = \begin{pmatrix} 0 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in I$, $rs_1 = \begin{pmatrix} 0 & ab_1 \\ 0 & 0 \end{pmatrix} \in I$ και $s_1r = \begin{pmatrix} 0 & b_1d \\ 0 & 0 \end{pmatrix} \in I$. Άρα το I είναι ιδεώδες του R .

Ας δείξουμε τώρα ότι $R/I \simeq \mathbb{Z} \times \mathbb{Z}$.

Θεωρούμε την απεικόνιση $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ με $\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = (a, d)$.

Παρατηρούμε ότι

(i) Η φ είναι ομομορφισμός. Πράγματι, εάν $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in R$, τότε $\varphi(r_1 + r_2) = (a_1 + a_2, d_1 + d_2) = (a_1, d_1) + (a_2, d_2) = \varphi(r_1) + \varphi(r_2)$ και $\varphi(r_1r_2) = (a_1a_2, d_1d_2) = (a_1, d_1)(a_2, d_2) = \varphi(r_1)\varphi(r_2)$.

(ii) Η φ είναι επί, αφού αν $(a, d) \in \mathbb{Z} \times \mathbb{Z}$, τότε για $r = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in R$ έχουμε $\varphi(r) = (a, d)$.

(iii) Τέλος, $\text{Ker } \varphi = I$. Πράγματι, εάν $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$, τότε $r \in \text{Ker } \varphi \iff \varphi(r) = (0, 0) \iff (a, d) = (0, 0) \iff a = 0 \text{ και } d = 0 \iff r \in I$.

Τώρα από το 1ο Θ.Ι.Δ., έχουμε ότι $R/\text{Ker } \varphi \simeq \text{Im } \varphi$ και εφόσον $\text{Ker } \varphi = I$ και $\text{Im } \varphi = \mathbb{Z} \times \mathbb{Z}$, έπεται ότι $R/I \simeq \mathbb{Z} \times \mathbb{Z}$.

(3) Το I δεν είναι πρώτο. Πράγματι, εάν $r_1 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ και $r_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, τότε $r_1r_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$, ενώ $r_1, r_2 \notin I$.

β' τρόπος

Αν το I ήταν πρώτο, τότε ο R/I δεν θα είχε μηδενοδιαιρέτες (πράγματι, εάν $(a + I)(b + I) = I$, τότε $ab \in I$, άρα $a \in I$ ή $b \in I$). Όμως $R/I \simeq \mathbb{Z} \times \mathbb{Z}$, και ο $\mathbb{Z} \times \mathbb{Z}$ έχει μηδενοδιαιρέτες, αφού $(1, 0), (0, 1) \neq (0, 0)$ και $(1, 0)(0, 1) = (0, 0)$. Άτοπο.

Άσκηση 54.

Θεωρούμε $R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ και $I = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{Z} \right\}$.

- (1) Δείξτε ότι ο R είναι υποδακτύλιος του $M_2(\mathbb{Z})$. Είναι ο R α.π.;
- (2) Δείξτε ότι το I είναι ιδεώδες του R και ότι $R/I \simeq \mathbb{Z}$.
- (3) Βρείτε όλα τα αντιστρέψιμα στοιχεία του R .
- (4) Είναι ο δακτύλιος R ισόμορφος με τον $\mathbb{Z} \times \mathbb{Z}$;

Λύση.

- (1) Εύκολα δείχνουμε ότι ο R είναι υποδακτύλιος του $M_2(\mathbb{Z})$. Ο R δεν είναι α.π.,

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

- (2) Εύκολα το I ιδεώδες. Θεωρούμε την απεικόνιση $\varphi : R \rightarrow \mathbb{Z}$ με

$$\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b.$$

- (i) Η φ είναι ομομορφισμός. Πράγματι, εάν $r_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, $r_2 = \begin{pmatrix} \delta & \varepsilon \\ \varepsilon & \delta \end{pmatrix} \in R$, τότε $\varphi(r_1 + r_2) = a + \delta - (b + \varepsilon) = (a - b) + (\delta - \varepsilon) = \varphi(r_1) + \varphi(r_2)$ και $\varphi(r_1 r_2) = a\delta + b\varepsilon - a\varepsilon - b\delta = (a - b)(\delta - \varepsilon) = \varphi(r_1)\varphi(r_2)$.

- (ii) Η φ είναι επί, διότι εάν $m \in \mathbb{Z}$, τότε $\varphi\left(\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}\right) = m$.

- (iii) $\text{Ker } \varphi = I$. Πράγματι εάν $r = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in R$, τότε

$$r \in \text{Ker } \varphi \iff \varphi(r) = 0 \iff a - b = 0 \iff a = b \iff r \in I.$$

Άρα, από το 1ο Θ.Ι.Δ., $R/I = R/\text{Ker } \varphi \simeq \text{Im } \varphi = \mathbb{Z}$.

- (3) Έστω $r = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in R$, τότε

$$r \in U(R) \xrightarrow{\text{γιατί;}} r \in U(M_2(\mathbb{Z})) \implies \det \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in U(\mathbb{Z}).$$

$$\implies a^2 - b^2 = 1 \text{ ή } -1$$

$$\implies a = \pm 1 \text{ και } b = 0 \quad \text{ή} \quad a = 0 \text{ και } b = \pm 1.$$

Οπότε

$$r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Οπότε

$$U(R) \subseteq \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Επειδή τώρα τα $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ ανήκουν στο $U(R)$, έχουμε ότι

$$U(R) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

(4) Έστω ότι υπάρχει $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ ισομορφισμός.

Εφόσον η φ είναι επιμορφισμός, έχουμε ότι $\varphi(1_R) = 1_{\mathbb{Z} \times \mathbb{Z}}$

Έστω $a \in \mathbb{Z}$. τότε

$$\varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) \stackrel{a1_R = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}}{=} \varphi(a1_R) \stackrel{2.6.3(5)}{=} a\varphi(1_R) = a1_{\mathbb{Z} \times \mathbb{Z}} = a(1, 1) = (a, a).$$

Οπότε

$$\varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = (a, a), \quad \text{για κάθε } a \in \mathbb{Z}.$$

Έστω ότι $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (x, y)$. Επειδή $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, έχουμε

$$(x^2, y^2) = \varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1, 1).$$

$$x^2 = 1, \quad y^2 = 1 \Rightarrow x = \pm 1 \text{ και } y = \pm 1.$$

Εάν $x = 1, y = 1$, τότε $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1, 1)$.

Ατοπο διότι η φ είναι 1-1 και $\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1, 1)$.

Εάν $x = -1, y = -1$, τότε $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (-1, -1)$.

$$\varphi\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1, 1) + (-1, -1) = (0, 0).$$

Ατοπο διότι αφού η φ είναι 1-1, $\text{Ker } \varphi = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

Έστω τώρα ότι $x = -1, y = 1$.

Τότε $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (-1, 1)$. Εάν $\beta \in \mathbb{Z}$, τότε

$$\varphi\left(\begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}\right) = \varphi\left(\beta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) \stackrel{2.6.3(5)}{=} \beta \varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = \beta(-1, 1) = (-\beta, \beta).$$

Επίσης εάν $r = \begin{pmatrix} a & \beta \\ \beta & a \end{pmatrix} \in R$, τότε

$$\varphi(r) = \varphi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}\right) = (a, a) + (-\beta, \beta) = (a - \beta, a + \beta).$$

Άτοπο εφόσον η φ είναι επί και δεν υπάρχουν $a, \beta \in \mathbb{Z}$ ώστε

$$(a - \beta, a + \beta) = (2, 3).$$

Ομοίως καταλήγουμε σ' άτοπο εάν $\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1, -1)$.

Άρα δεν υπάρχει $\varphi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ ισομορφισμός.

Άσκηση 55.

Έστω $R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$ και $I = \left\{ \begin{pmatrix} 3a & b \\ 0 & 2d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}$.

(1) Δείξτε ότι ο R είναι υποδακτύλιος του $M_2(\mathbb{Z})$ και το I ιδεώδες του R . Είναι το I ιδεώδες του $M_2(\mathbb{Z})$;

(2) Δείξτε ότι $R/I \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$. Είναι το I πρώτο ή μεγιστικό ιδεώδες του R ;

Λύση.

(1) Καταρχάς $R \neq \emptyset$. Επίσης, εάν $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in R$, τότε $r_1 + r_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & d_1 + d_2 \end{pmatrix} \in R$, $r_1 r_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \in R$ και $-r_1 = \begin{pmatrix} -a_1 & -b_1 \\ 0 & -d_1 \end{pmatrix} \in R$. Άρα ο R είναι υποδακτύλιος του $M_2(\mathbb{Z})$.

Ας δείξουμε τώρα ότι το I είναι ιδεώδες του R . Καταρχάς $I \neq \emptyset$. Έστω

$r_1 = \begin{pmatrix} 3a_1 & b_1 \\ 0 & 2d_1 \end{pmatrix}$, $r_2 = \begin{pmatrix} 3a_2 & b_2 \\ 0 & 2d_2 \end{pmatrix} \in I$ και $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$. Τότε $r_1 - r_2 = \begin{pmatrix} 3(a_1 - a_2) & b_1 - b_2 \\ 0 & 2(d_1 - d_2) \end{pmatrix} \in I$, $rr_1 = \begin{pmatrix} 3aa_1 & ab_1 + 2bd_1 \\ 0 & 2dd_1 \end{pmatrix} \in I$ και ομοίως $r_1 r \in I$.

Άρα το I είναι ιδεώδες του R .

Το I δεν είναι ιδεώδες του $M_2(\mathbb{Z})$, διότι εάν ήταν, τότε για $r = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$

και $r_1 = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \in I$ θα έπρεπε $rr_1 \in I$. Όμως $rr_1 = \begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix} \notin I$. Άτοπο.

(2) Έστω η $\varphi : R \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_2$ με $\varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = ([a]_3, [d]_2)$.

Έχουμε ότι

(i) Η φ είναι ομομορφισμός δακτυλίων.

Πράγματι, έστω $r_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $r_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in R$, τότε

$$\begin{aligned} \varphi(r_1 + r_2) &= \varphi\left(\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & d_1 + d_2 \end{pmatrix}\right) = ([a_1 + a_2]_3, [d_1 + d_2]_2) = ([a_1]_3, [d_1]_2) + \\ &([a_2]_3, [d_2]_2) = \varphi(r_1) + \varphi(r_2) \end{aligned}$$

και

$$\begin{aligned} \varphi(r_1 r_2) &= \varphi\left(\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}\right) = ([a_1 a_2]_3, [d_1 d_2]_2) = ([a_1]_3, [d_1]_2) \cdot ([a_2]_3, [d_2]_2) = \\ &\varphi(r_1) \varphi(r_2). \end{aligned}$$

(ii) Η φ είναι επί.

Πράγματι, έστω $([a]_3, [d]_2) \in \mathbb{Z}_3 \times \mathbb{Z}_2$. Τότε για $r = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in R$ έχουμε $\varphi(r) = ([a]_3, [d]_2)$.

(iii) $\text{Ker } \varphi = I$.

Πράγματι, έστω $r = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R$. Τότε

$$r \in \text{Ker } \varphi \iff \varphi(r) = 0_{\mathbb{Z}_3 \times \mathbb{Z}_2} \iff ([a]_3, [d]_2) = ([0]_3, [0]_2) \iff 3 \mid a \text{ και } 2 \mid d \iff r \in I.$$

Τώρα από το 1ο Θ.Ι.Δ. έχουμε ότι

$$R / \text{Ker } \varphi \simeq \text{Im } \varphi \xrightarrow[\text{Ker } \varphi = I]{\text{Im } \varphi = \mathbb{Z}_3 \times \mathbb{Z}_2} R / I \simeq \mathbb{Z}_3 \times \mathbb{Z}_2.$$

Τέλος παρατηρούμε ότι ο R/I δεν είναι α.π., διότι $R/I \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$, και ο $\mathbb{Z}_3 \times \mathbb{Z}_2$ δεν είναι α.π. αφού

$$([0]_3, [1]_2) \cdot ([1]_3, [0]_2) = ([0]_3, [0]_2), \quad ([0]_3, [1]_2), ([1]_3, [0]_2) \neq ([0]_3, [0]_2).$$

Οπότε ο R/I έχει μηδενοδιαιρέτες. Επομένως το I δεν είναι πρώτο, διότι, εάν ήταν, τότε από $(a+I)(b+I) = I$ θα είχαμε $ab \in I$, άρα $a \in I$ ή $b \in I$, δηλαδή ο R/I δεν θα είχε μηδενοδιαιρέτες.

Το I δεν είναι ούτε μεγιστικό. Εδώ ο R δεν είναι μεταθετικός, οπότε δεν εφαρμόζεται το Θεώρημα 2.9.3. Δίνουμε ένα ενδιάμεσο ιδεώδες. Έστω

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 2d \end{pmatrix} : a, b, d \in \mathbb{Z} \right\}.$$

Το J είναι ιδεώδες του R , ως πυρήνας του ομομορφισμού $\psi : R \rightarrow \mathbb{Z}_2$ με

$$\psi \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) = [d]_2.$$

Επίσης $I \subsetneq J \subsetneq R$, αφού

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in J \setminus I \quad \text{και} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R \setminus J.$$

Άρα το I δεν είναι μεγιστικό.

Άσκηση 56.

Έστω R ο δακτύλιος των άνω τριγωνικών 3×3 πινάκων και $S, I \subseteq R$ με

$$S = \left\{ \begin{pmatrix} a & 0 & \delta \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix} : a, b, \gamma, \delta \in \mathbb{C} \right\}, \quad I = \left\{ \begin{pmatrix} 0 & 0 & \delta \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : \delta \in \mathbb{C} \right\}.$$

- (1) Δείξτε ότι ο S είναι υποδακτύλιος του R . Είναι ο R μεταθετικός;
- (2) Δείξτε ότι το I είναι ιδεώδες του S . Είναι το I ιδεώδες του R ;
- (3) Δείξτε ότι $S/I \simeq \mathbb{C} \times \mathbb{C} \times \mathbb{C}$.

Λύση.

(1) Καταρχάς έχουμε ότι $R = \left\{ \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & a_5 \\ 0 & 0 & a_6 \end{pmatrix} : a_i \in \mathbb{C}, i = 1, \dots, 6 \right\}.$

Ο R δεν είναι μεταθετικός, διότι για $r_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, r_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in R$ έχουμε

$$r_1 r_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{ ενώ } r_2 r_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \text{ άρα } r_1 r_2 \neq r_2 r_1.$$

Τώρα για τον S καταρχάς παρατηρούμε ότι $S \neq \emptyset$.

Επίσης εάν $s_1 = \begin{pmatrix} a_1 & 0 & \delta_1 \\ 0 & b_1 & 0 \\ 0 & 0 & \gamma_1 \end{pmatrix}, s_2 = \begin{pmatrix} a_2 & 0 & \delta_2 \\ 0 & b_2 & 0 \\ 0 & 0 & \gamma_2 \end{pmatrix} \in S$ και $s = \begin{pmatrix} a & 0 & \delta \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix}$, τότε

$$s_1 + s_2 = \begin{pmatrix} a_1 + a_2 & 0 & \delta_1 + \delta_2 \\ 0 & b_1 + b_2 & 0 \\ 0 & 0 & \gamma_1 + \gamma_2 \end{pmatrix} \in S, \quad s_1 s_2 = \begin{pmatrix} a_1 a_2 & 0 & a_1 \delta_2 + \delta_1 \gamma_2 \\ 0 & b_1 b_2 & 0 \\ 0 & 0 & \gamma_1 \gamma_2 \end{pmatrix} \in S \text{ και}$$

$$-s = \begin{pmatrix} -a & 0 & -\delta \\ 0 & -b & 0 \\ 0 & 0 & -\gamma \end{pmatrix} \in S.$$

Άρα ο S είναι υποδακτύλιος του R .

(2) Καταρχάς $I \neq \emptyset$. Το I είναι ιδεώδες του S διότι εάν $t_1 = \begin{pmatrix} 0 & 0 & \delta_1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$

$$t_2 = \begin{pmatrix} 0 & 0 & \delta_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I \text{ και } s = \begin{pmatrix} a & 0 & \delta \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix} \in S, \text{ τότε } t_1 - t_2 = \begin{pmatrix} 0 & 0 & \delta_1 - \delta_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I,$$

$$t_1 s, s t_1 \in I.$$

Αφήνεται ως άσκηση ο έλεγχος αν το I είναι ιδεώδες του R .

(3) Θεωρούμε την απεικόνιση $\varphi : S \rightarrow \mathbb{C} \times \mathbb{C} \times \mathbb{C}$ με $\varphi \left(\begin{pmatrix} a & 0 & \delta \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix} \right) = (a, b, \gamma)$.

(i) Η φ είναι ομομορφισμός.

Πράγματι, έστω $s_1 = \begin{pmatrix} a_1 & 0 & \delta_1 \\ 0 & b_1 & 0 \\ 0 & 0 & \gamma_1 \end{pmatrix}, s_2 = \begin{pmatrix} a_2 & 0 & \delta_2 \\ 0 & b_2 & 0 \\ 0 & 0 & \gamma_2 \end{pmatrix} \in S$. Τότε εύκολα διαπιστώνουμε ότι $\varphi(s_1 + s_2) = \varphi(s_1) + \varphi(s_2)$ και $\varphi(s_1 s_2) = \varphi(s_1) \varphi(s_2)$.

(ii) Η φ είναι επί, διότι εάν $(a, b, \gamma) \in \mathbb{C} \times \mathbb{C} \times \mathbb{C}$, τότε για $s = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix} \in S$

έχουμε $\varphi(s) = (a, b, \gamma)$.

(iii) $\text{Ker } \varphi = I$. Πράγματι, εάν $s = \begin{pmatrix} a & 0 & \delta \\ 0 & b & 0 \\ 0 & 0 & \gamma \end{pmatrix} \in S$, τότε

$$s \in \text{Ker } \varphi \iff \varphi(s) = (0, 0, 0) \iff (a, b, \gamma) = (0, 0, 0) \iff a = b = \gamma = 0 \iff s \in I.$$

Άρα, από το 1ο Θ.Ι.Δ., $S/I \simeq \text{Im } \varphi = \mathbb{C} \times \mathbb{C} \times \mathbb{C}$.

Άσκηση 57.

Έστω R πεπερασμένος δακτύλιος με $|R| > 1$. Δείξτε ότι εάν υπάρχει επιμορφισμός $\varphi : \mathbb{Z} \rightarrow R$, τότε ο R είναι ισόμορφος με τον $\mathbb{Z}_m$, για κάποιο θετικό ακέραιο m .

Λύση.

Καταρχάς από το 1ο Θ.Ι.Δ. έχουμε ότι

$$\mathbb{Z} / \text{Ker } \varphi \simeq \text{Im } \varphi \stackrel{\varphi \text{ επί}}{=} R. \quad (1)$$

Επίσης, εφόσον η φ είναι ομομορφισμός, έπεται ότι $\text{Ker } \varphi$ ιδεώδες του $\mathbb{Z}$. Επειδή κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο, υπάρχει $m \geq 0$ ώστε $\text{Ker } \varphi = \langle m \rangle$.

Θα δείξουμε ότι $m \neq 0$.

Πράγματι, εάν $m = 0$, τότε $\text{Ker } \varphi = \{0\}$, άρα η φ είναι 1-1. Επομένως εφόσον το $\mathbb{Z}$ είναι άπειρο, άπειρη θα είναι και η $\text{Im } \varphi = \varphi(\mathbb{Z})$. Άτοπο εφόσον το R πεπερασμένο.

Συνεπώς υπάρχει $m > 0$ ώστε $\text{Ker } \varphi = \langle m \rangle$.

Θα δείξουμε ότι $\mathbb{Z} / \langle m \rangle \simeq \mathbb{Z}_m$. (2)

Πράγματι, έστω η $\psi : \mathbb{Z} \rightarrow \mathbb{Z}_m$ με $\psi(a) = [a]$.

Τότε η ψ είναι ομομορφισμός (γιατί;) και επί, αφού

$$\psi(\mathbb{Z}) = \{\psi(a) : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\} = \mathbb{Z}_m.$$

Επίσης, $\text{Ker } \psi = \langle m \rangle$ διότι, εάν $a \in \mathbb{Z}$, τότε

$$a \in \text{Ker } \psi \iff \psi(a) = [0] \iff [a] = [0] \iff m \mid a.$$

Τέλος από το 1ο Θ.Ι.Δ. έχουμε ότι

$$\mathbb{Z} / \text{Ker } \psi \simeq \text{Im } \psi \stackrel{\text{Ker } \psi = \langle m \rangle}{=} \mathbb{Z} / \langle m \rangle \simeq \mathbb{Z}_m.$$

Από τις (1), (2), δεδομένου ότι $\text{Ker } \varphi = \langle m \rangle$, έχουμε

$$\mathbb{Z} / \langle m \rangle \simeq R \quad \text{και} \quad \mathbb{Z} / \langle m \rangle \simeq \mathbb{Z}_m.$$

Άρα $R \simeq \mathbb{Z}_m$.

Άσκηση 58.

Έστω $n, m \in \mathbb{Z}_{>0}$ με $n, m \geq 2$ και $I = \langle n \rangle \times \langle m \rangle$.

(1) Δείξτε ότι το I είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$.

(2) Δείξτε ότι $(\mathbb{Z} \times \mathbb{Z})/I \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.

Λύση.

(1) Θα αποδείξουμε κάτι γενικότερο. Το εξής:

Αν R, S δακτύλιοι, I_1, I_2 ιδεώδη των R, S αντίστοιχα, τότε το $I_1 \times I_2$ είναι ιδεώδες του $R \times S$.

Πράγματι, καταρχάς εφόσον I_1, I_2 ιδεώδη, $I_1, I_2 \neq \emptyset$, άρα $I_1 \times I_2 \neq \emptyset$.

Έστω $(a_1, b_1), (a_2, b_2) \in I_1 \times I_2$. Τότε $(a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \in I_1 \times I_2$, διότι αφού I_1 ιδεώδες, $a_1, a_2 \in I_1 \Rightarrow a_1 - a_2 \in I_1$ και ομοίως $b_1 - b_2 \in I_2$.

Επίσης εάν $(a, b) \in I_1 \times I_2, (r, s) \in R \times S$, τότε $(r, s) \cdot (a, b) = (ra, sb) \in I_1 \times I_2$, διότι αφού I_1, I_2 ιδεώδη των R, S αντίστοιχα, $r \in R, s \in S, a \in I_1, b \in I_2$ έπεται ότι $ra \in I_1, sb \in I_2$.

Ομοίως $(a, b)(r, s) \in I_1 \times I_2$.

Άρα για $I_1 = \langle n \rangle, I_2 = \langle m \rangle$, εφόσον τα I_1, I_2 είναι ιδεώδη του $\mathbb{Z}$, έπεται ότι $I = I_1 \times I_2$ είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$.

(2) Έστω η $\varphi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m$ με $\varphi((a, b)) = ([a]_n, [b]_m), a, b \in \mathbb{Z}$.

Έχουμε ότι

(i) φ ομομορφισμός.

Πράγματι, εάν $(a_1, b_1), (a_2, b_2) \in \mathbb{Z} \times \mathbb{Z}$, τότε

$$\begin{aligned}\varphi((a_1, b_1) + (a_2, b_2)) &= \varphi((a_1 + a_2, b_1 + b_2)) \\ &= ([a_1 + a_2]_n, [b_1 + b_2]_m) \\ &= ([a_1]_n, [b_1]_m) + ([a_2]_n, [b_2]_m) \\ &= \varphi((a_1, b_1)) + \varphi((a_2, b_2)).\end{aligned}$$

Όμοια $\varphi((a_1, b_1) \cdot (a_2, b_2)) = \varphi((a_1, b_1)) \cdot \varphi((a_2, b_2))$.

(ii) $\text{Ker } \varphi = \langle n \rangle \times \langle m \rangle = I$.

Πράγματι, εάν $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, τότε

$$\begin{aligned}(a, b) \in \text{Ker } \varphi &\iff \varphi((a, b)) = ([0]_n, [0]_m) \iff ([a]_n, [b]_m) = ([0]_n, [0]_m) \\ &\iff [a]_n = [0]_n \text{ και } [b]_m = [0]_m \iff n \mid a \text{ και } m \mid b \\ &\iff a \in \langle n \rangle \text{ και } b \in \langle m \rangle \iff (a, b) \in I.\end{aligned}$$

(iii) φ επί.

Πράγματι

$$\operatorname{Im} \varphi = \{\varphi((a, b)) : a, b \in \mathbb{Z}\} = \{([a]_n, [b]_m) : a, b \in \mathbb{Z}\} = \mathbb{Z}_n \times \mathbb{Z}_m.$$

Τέλος, από το 1ο Θ.Ι.Δ. έχουμε

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

Άσκηση

Δείξτε ότι $I = \{(2k, 3\ell) : k, \ell \in \mathbb{Z}\}$ είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ και ότι $(\mathbb{Z} \times \mathbb{Z})/I \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$.

Άσκηση 59.

Έστω $m \in \mathbb{Z}$ με $m \geq 2$, $R = M_n(\mathbb{Z})$, $J = M_n(I)$, όπου $I = \langle m \rangle$. Αποδείξτε ότι:

(1) J ιδεώδες του R .

(2) $R/J \simeq M_n(\mathbb{Z}_m)$.

Λύση.

(1) Προφανώς $J \neq \emptyset$, αφού $I \neq \emptyset$.

Έστω $A = (a_{ij})$, $B = (b_{ij}) \in J$. Τότε $A - B = (a_{ij} - b_{ij})$ και $a_{ij} - b_{ij} \in I$ για κάθε $i, j = 1, \dots, n$, αφού I ιδεώδες του $\mathbb{Z}$. Άρα $A - B \in J$.

Έστω $A \in R$, $B \in J$. Εφόσον $J = M_n(I)$ και $I = \langle m \rangle$, υπάρχει $\Gamma \in M_n(\mathbb{Z})$ ώστε $B = m\Gamma$. Οπότε $AB = m(A\Gamma) \in J$ και $BA = m(\Gamma A) \in J$.

Άρα J είναι ιδεώδες του R .

(2) Ορίζουμε $\varphi : M_n(\mathbb{Z}) \rightarrow M_n(\mathbb{Z}_m)$ με

$$\varphi((a_{ij})) = ([a_{ij}]),$$

όπου $A = (a_{ij}) \in M_n(\mathbb{Z})$.

Η φ είναι ομομορφισμός δακτυλίων.

Πράγματι, αν $A = (a_{ij})$, $B = (b_{ij}) \in M_n(\mathbb{Z})$ και $AB = \Delta = (\delta_{ij})$, τότε $\varphi(A + B) = ([a_{ij} + b_{ij}]) = ([a_{ij}]) + ([b_{ij}]) = \varphi(A) + \varphi(B)$ και $\varphi(AB) = \varphi(\Delta) = ([\delta_{ij}]) = ([a_{ij}])([b_{ij}]) = \varphi(A)\varphi(B)$.

Επίσης, $\text{Ker } \varphi = M_n(I) = J$. Πράγματι, αν $A = (a_{ij}) \in M_n(\mathbb{Z})$, τότε $A \in \text{Ker } \varphi$ αν και μόνο αν $\varphi(A) = ([a_{ij}]) = 0$, αν και μόνο αν $[a_{ij}] = [0]$ για κάθε $i, j = 1, \dots, n$, αν και μόνο αν $m \mid a_{ij}$ για κάθε $i, j = 1, \dots, n$, αν και μόνο αν $A = (a_{ij}) \in M_n(I)$.

Η φ επίσης είναι επί (γιατί;).

Τέλος απο το 1ο Θ.Ι.Δ. έχουμε

$$R/J = R/\text{Ker } \varphi \simeq \text{Im } \varphi = M_n(\mathbb{Z}_m).$$

Άσκηση 60.

Έστω p πρώτος και

$$R_p = \left\{ \frac{m}{n} \in \mathbb{Q} : p \nmid n \right\}, \quad I_p = \left\{ \frac{m}{n} \in \mathbb{Q} : p \nmid n, p \mid m \right\}.$$

Να δειχθεί ότι:

(1) Το R_p είναι δακτύλιος με τις συνήθεις πράξεις.

(2) Το I_p είναι ιδεώδες του R_p .

(3) $R_p/I_p \simeq \mathbb{Z}_p$.

Λύση.

Παρατήρηση. Κάθε $x \in \mathbb{Q}$ γράφεται $x = \frac{m_0}{n_0}$ με $(m_0, n_0) = 1$, $n_0 > 0$, και, εάν $x = \frac{m}{n}$ είναι οποιαδήποτε άλλη γραφή του, τότε $m = km_0$, $n = kn_0$ για κάποιο $k \in \mathbb{Z}$. Επομένως, εάν $p \nmid n$, τότε $p \nmid k$ και $p \nmid n_0$, οπότε $p \mid m \iff p \mid m_0$. Άρα οι συνθήκες που ορίζουν τα R_p , I_p δεν εξαρτώνται από τη γραφή $\frac{m}{n}$ που επιλέγουμε (με $p \nmid n$).

(1) Θα δείξουμε ότι το R_p είναι υποδακτύλιος του $\mathbb{Q}$ και άρα δακτύλιος.

Προφανώς $R_p \neq \emptyset$. Έστω $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in R_p$.

Τότε $\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1n_2 + m_2n_1}{n_1n_2}$.

Το $p \nmid n_1n_2$, διότι αν $p \mid n_1n_2$, τότε αφού το p είναι πρώτος, θα είχαμε $p \mid n_1$ ή $p \mid n_2$, άτοπο. Άρα $\frac{m_1}{n_1} + \frac{m_2}{n_2} \in R_p$.

Ομοίως, $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1m_2}{n_1n_2} \in R_p$.

Τέλος, $-\frac{m_1}{n_1} = \frac{-m_1}{n_1} \in R_p$.

(2) Καταρχάς $I_p \neq \emptyset$, αφού $\frac{p}{1} \in I_p$.

Έστω $x_1 = \frac{m_1}{n_1}$, $x_2 = \frac{m_2}{n_2} \in I_p$. Τότε

$$x_1 - x_2 = \frac{m_1n_2 - m_2n_1}{n_1n_2}.$$

Επειδή $x_1, x_2 \in I_p$, έχουμε $p \mid m_1$ και $p \mid m_2$, οπότε $p \mid m_1n_2 - m_2n_1$. Επίσης, αφού $p \nmid n_1$ και $p \nmid n_2$, έχουμε $p \nmid n_1n_2$. Άρα $x_1 - x_2 \in I_p$.

Έστω τώρα $x = \frac{m}{n} \in R_p$ και $s = \frac{k}{\lambda} \in I_p$. Τότε

$$xs = \frac{mk}{n\lambda}.$$

Επειδή $s \in I_p$, έχουμε $p \mid k$, άρα $p \mid mk$. Επίσης, επειδή $x \in R_p$ και $s \in I_p$, έχουμε $p \nmid n$ και $p \nmid \lambda$, οπότε $p \nmid n\lambda$. Άρα $xs \in I_p$. Ομοίως $sx \in I_p$.

Επομένως I_p είναι ιδεώδες του R_p .

(3) Θα δούμε πρώτα ποιο είναι το "χαρακτηριστικό" που διακρίνει δύο κλάσεις του R_p/I_p .

Έστω $\frac{m}{n} + I_p, \frac{k}{\lambda} + I_p \in R_p/I_p$. Επειδή $\frac{m}{n}, \frac{k}{\lambda} \in R_p$, έχουμε $p \nmid n$ και $p \nmid \lambda$, άρα $[n], [\lambda] \in U(\mathbb{Z}_p)$.

Επίσης

$$\frac{m}{n} + I_p = \frac{k}{\lambda} + I_p \Leftrightarrow \frac{m\lambda - kn}{n\lambda} \in I_p \Leftrightarrow p \mid m\lambda - kn. \Leftrightarrow [m][\lambda] = [k][n] \Leftrightarrow [m][n]^{-1} = [k][\lambda]^{-1}.$$

Άρα

$$\frac{m}{n} + I_p \neq \frac{k}{\lambda} + I_p \Leftrightarrow [m][n]^{-1} \neq [k][\lambda]^{-1}.$$

Ορίζουμε $\varphi : R_p \rightarrow \mathbb{Z}_p$ με $\varphi\left(\frac{m}{n}\right) = [m][n]^{-1}$.

Η φ είναι καλά ορισμένη, διότι, εάν $\frac{m}{n} = \frac{k}{\lambda}$, τότε $m\lambda - kn = 0$, οπότε $p \mid m\lambda - kn$ και, από τα παραπάνω, $[m][n]^{-1} = [k][\lambda]^{-1}$.

Η φ είναι ομομορφισμός δακτυλίων, διότι

$$\varphi\left(\frac{m}{n} + \frac{k}{\lambda}\right) = \varphi\left(\frac{m\lambda + kn}{n\lambda}\right) = [m\lambda + kn][n\lambda]^{-1} = [m][n]^{-1} + [k][\lambda]^{-1} = \varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{k}{\lambda}\right)$$

και

$$\varphi\left(\frac{m}{n} \cdot \frac{k}{\lambda}\right) = [mk][n\lambda]^{-1} = [m][n]^{-1}[k][\lambda]^{-1} = \varphi\left(\frac{m}{n}\right) \varphi\left(\frac{k}{\lambda}\right).$$

Επίσης $\text{Ker } \varphi = I_p$, διότι

$$\varphi\left(\frac{m}{n}\right) = [0] \iff [m][n]^{-1} = [0] \iff [m] = [0] \iff p \mid m \iff \frac{m}{n} \in I_p.$$

Τέλος, η φ είναι επί, αφού για κάθε $[k] \in \mathbb{Z}_p$ υπάρχει $\frac{k}{1} \in R_p$ ώστε $\varphi\left(\frac{k}{1}\right) = [k]$.

Άρα, από το 1ο Θ.Ι.Δ. έχουμε ότι $R_p/\text{Ker } \varphi \simeq \text{Im } \varphi$, οπότε $R_p/I_p \simeq \mathbb{Z}_p$.

Παρατήρηση

Αξίζει να παρατηρήσουμε ότι:

(1) $\mathbb{Z} \subseteq R_p$, διότι αν $m \in \mathbb{Z}$, τότε $m = \frac{m}{1}$ και $p \nmid 1$.

(2) Αν $\psi = \varphi|_{\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}_p$, τότε $\psi(m) = [m]$ για κάθε $m \in \mathbb{Z}$.

Άσκηση 61.

Έστω

$$R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{2}].$$

- (1) Δείξτε ότι ο R είναι ακέραια περιοχή αλλά όχι σώμα.
- (2) Αν $\langle 5 \rangle = \{5t : t \in R\} = \{5a + 5b\sqrt{2} : a, b \in \mathbb{Z}\}$, δείξτε ότι το $R/\langle 5 \rangle$ είναι σώμα.
- (3) Δείξτε ότι $|R/\langle 5 \rangle| = 5^2$.

Λύση.

- (1) Έστω $z_1 = a + b\sqrt{2}$, $z_2 = \gamma + \delta\sqrt{2} \in R$ με $z_1 z_2 = 0$. Τότε

$$(a\gamma + 2b\delta) + (a\delta + b\gamma)\sqrt{2} = 0,$$

οπότε

$$a\gamma + 2b\delta = 0 \quad \text{και} \quad a\delta + b\gamma = 0.$$

Έστω $z_1 \neq 0$, δηλαδή $a \neq 0$ ή $b \neq 0$. Θεωρούμε το σύστημα

$$\gamma x + 2\delta y = 0, \quad \delta x + \gamma y = 0.$$

Το σύστημα αυτό έχει τη μη τετριμμένη λύση $x = a$, $y = b$, άρα η ορίζουσά του είναι μηδέν. Επομένως

$$\begin{vmatrix} \gamma & 2\delta \\ \delta & \gamma \end{vmatrix} = 0 \Rightarrow \gamma^2 - 2\delta^2 = 0.$$

Άρα $\gamma^2 = 2\delta^2$, δηλαδή $|\gamma| = \sqrt{2}|\delta|$, πράγμα αδύνατο για $\gamma, \delta \in \mathbb{Z}$, εκτός αν $\gamma = \delta = 0$.

Επομένως $z_2 = 0$. Ομοίως, αν $z_2 \neq 0$, τότε $z_1 = 0$. Άρα ο R είναι ακέραια περιοχή. Αν ο R ήταν σώμα, τότε το στοιχείο $2 = 2 + 0\sqrt{2} \in R$ θα ήταν αντιστρέψιμο. Θα υπήρχε δηλαδή $z = a + b\sqrt{2} \in R$ ώστε

$$2z = 1 \Rightarrow 2a + 2b\sqrt{2} = 1.$$

Άρα $2a = 1$, άτοπο, αφού $a \in \mathbb{Z}$.

Επομένως ο R δεν είναι σώμα.

- (2) Θέτουμε $I = \langle 5 \rangle$.

Ο R/I είναι μεταθετικός με μοναδιαίο το $1 + I$, και $1 + I \neq I = 0_{R/I}$, αφού $1 \notin I$ (διότι $5 \nmid 1$). Αρκεί λοιπόν να δείξουμε ότι κάθε μη μηδενικό στοιχείο του R/I είναι αντιστρέψιμο.

Καταρχάς, αν $z = a + b\sqrt{2} \in R$, τότε

$$z + I = 0_{R/I} \Leftrightarrow z \in I \Leftrightarrow a + b\sqrt{2} = 5\gamma + 5\delta\sqrt{2}$$

για κάποια $\gamma, \delta \in \mathbb{Z}$, δηλαδή

$$z + I = 0_{R/I} \Leftrightarrow 5 \mid a \text{ και } 5 \mid b \Leftrightarrow [a] = [0] \text{ και } [b] = [0] \text{ στη } \mathbb{Z}_5.$$

Έστω $z = a + b\sqrt{2} \in R$ με $z + I \neq 0_{R/I}$. Τότε $[a] \neq [0]$ ή $[b] \neq [0]$ στη $\mathbb{Z}_5$.

Θα δείξουμε ότι υπάρχει $x + y\sqrt{2} \in R$ ώστε $(z + I)((x + y\sqrt{2}) + I) = 1 + I$. Η ισότητα αυτή ισοδυναμεί με

$$(ax + 2by - 1) + (ay + bx)\sqrt{2} \in I,$$

δηλαδή με το σύστημα

$$\begin{cases} [a][x] + [2b][y] = [1], \\ [b][x] + [a][y] = [0] \end{cases}$$

στη $\mathbb{Z}_5$.

Η ορίζουσα του συστήματος είναι

$$\Delta = \begin{vmatrix} [a] & [2b] \\ [b] & [a] \end{vmatrix} = [a^2 - 2b^2].$$

Θα δείξουμε ότι $\Delta \neq [0]$. Αν $\Delta = [0]$, τότε $[a^2] = [2b^2]$. Αν $[b] = [0]$, τότε $[a^2] = [0]$, άρα $[a] = [0]$, άτοπο. Αν $[b] \neq [0]$, τότε $([a][b]^{-1})^2 = [2]$, δηλαδή το $[2]$ είναι τετράγωνο στο $\mathbb{Z}_5$, άτοπο, αφού τα τετράγωνα στο $\mathbb{Z}_5$ είναι $[0], [1], [4]$.

Άρα $\Delta \neq [0]$. Επειδή το $\mathbb{Z}_5$ είναι σώμα, το σύστημα έχει λύση στη $\mathbb{Z}_5$. Επομένως υπάρχει $x + y\sqrt{2} \in R$ ώστε $(z + I)((x + y\sqrt{2}) + I) = 1 + I$.

Άρα κάθε μη μηδενικό στοιχείο του R/I είναι αντιστρέψιμο. Επομένως το R/I είναι σώμα.

(3) Θα δείξουμε ότι κάθε κλάση του R/I έχει μοναδικό αντιπρόσωπο της μορφής $a + b\sqrt{2}$, όπου $a, b \in \{0, 1, 2, 3, 4\}$.

Έστω $z = a + b\sqrt{2} \in R$. Γράφουμε $a = 5q + r$ και $b = 5q' + r'$, όπου $r, r' \in \{0, 1, 2, 3, 4\}$. Τότε

$$z = (r + r'\sqrt{2}) + 5(q + q'\sqrt{2}),$$

οπότε

$$z + I = (r + r'\sqrt{2}) + I.$$

Αν τώρα

$$(r + r'\sqrt{2}) + I = (s + s'\sqrt{2}) + I,$$

όπου $r, r', s, s' \in \{0, 1, 2, 3, 4\}$, τότε

$$(r - s) + (r' - s')\sqrt{2} \in I,$$

άρα

$$5 \mid (r - s) \quad \text{και} \quad 5 \mid (r' - s').$$

Επειδή $r, s, r', s' \in \{0, 1, 2, 3, 4\}$, έπεται ότι $r = s$ και $r' = s'$.

Άρα οι κλάσεις του R/I είναι ακριβώς οι

$$a + b\sqrt{2} + I, \quad a, b \in \{0, 1, 2, 3, 4\}.$$

Επομένως

$$|R/I| = 5^2 = 25.$$

Άσκηση 62.

Έστω m, n θετικοί ακέραιοι και $\varphi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ με $\varphi([a]_{mn}) = ([a]_m, [a]_n)$.

- (1) Δείξτε ότι η φ είναι ομομορφισμός.
- (2) Δείξτε ότι η φ είναι ισομορφισμός αν $(m, n) = 1$.
- (3) Αν $(m, n) = 1$, δείξτε ότι $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.
- (4) Αποδείξτε την πολλαπλασιαστικότητα της συνάρτησης του Euler.

Λύση.

(1) Καταρχάς η φ είναι καλά ορισμένη, διότι αν $[a]_{mn} = [b]_{mn}$, τότε $mn \mid a - b$, άρα $m \mid a - b$ και $n \mid a - b$. Επομένως $[a]_m = [b]_m$ και $[a]_n = [b]_n$, άρα $([a]_m, [a]_n) = ([b]_m, [b]_n)$.

Έπειτα η φ είναι ομομορφισμός, διότι αν $[a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}$, τότε

$$\begin{aligned}\varphi([a]_{mn} + [b]_{mn}) &= \varphi([a + b]_{mn}) \\ &= ([a + b]_m, [a + b]_n) \\ &= ([a]_m + [b]_m, [a]_n + [b]_n) \\ &= ([a]_m, [a]_n) + ([b]_m, [b]_n) \\ &= \varphi([a]_{mn}) + \varphi([b]_{mn}).\end{aligned}$$

Ομοίως $\varphi([a]_{mn}[b]_{mn}) = \varphi([a]_{mn})\varphi([b]_{mn})$.

(2) ($\Leftarrow$) Γνωρίζουμε ότι εάν X, Y πεπερασμένα σύνολα με $|X| = |Y|$ και $f : X \rightarrow Y$. Τότε η f είναι επί ανν είναι 1-1.

Οπότε αρκεί να δείξουμε ότι η φ είναι 1-1 ή επί. Εδώ θα δείξουμε ότι είναι 1-1.

Αρκεί να δείξουμε ότι $\text{Ker } \varphi = \{[0]_{mn}\}$.

Έστω $[a]_{mn} \in \text{Ker } \varphi$. Τότε $\varphi([a]_{mn}) = ([0]_m, [0]_n)$, άρα $([a]_m, [a]_n) = ([0]_m, [0]_n)$, οπότε $[a]_m = [0]_m$ και $[a]_n = [0]_n$.

Άρα $m \mid a$ και $n \mid a$. Επειδή $(m, n) = 1$, έχουμε $mn \mid a$, οπότε $[a]_{mn} = [0]_{mn}$.

Άρα $\text{Ker } \varphi = \{[0]_{mn}\}$ και η φ είναι 1-1.

Τώρα έχουμε

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

Επειδή η φ είναι 1-1, έπεται ότι η φ είναι επί και επομένως ισομορφισμός.

($\Rightarrow$) Έστω ότι $d = (m, n) > 1$.

Παρατηρούμε ότι

$$\begin{aligned}\varphi\left(\left[\frac{mn}{d}\right]_{mn}\right) &= \left(\left[\frac{mn}{d}\right]_m, \left[\frac{mn}{d}\right]_n\right) \\ &= \left(\left[m\frac{n}{d}\right]_m, \left[\frac{m}{d}n\right]_n\right) \\ &= ([0]_m, [0]_n).\end{aligned}$$

Οπότε $\left[\frac{mn}{d}\right]_{mn} \in \text{Ker } \varphi$.

Επίσης $\left[\frac{mn}{d}\right]_{mn} \neq [0]_{mn}$, διότι αν $mn \mid \frac{mn}{d}$, τότε $\frac{mn}{d} = kmn$ για κάποιο $k \in \mathbb{Z}$, άρα $1 = kd$, άτοπο αφού $d > 1$.

Άρα $\text{Ker } \varphi \neq \{[0]_{mn}\}$, οπότε η φ δεν είναι 1-1, άτοπο.

Επομένως $(m, n) = 1$.

(3) Άμεσο από το (2), εφόσον $(m, n) = 1$, άρα η φ είναι ισομορφισμός και επομένως $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

(4) Έστω $(m, n) = 1$. Συμβολίζουμε εδώ τη συνάρτηση του Euler με ϕ , για να μη συγχέεται με τον ισομορφισμό φ . Δηλαδή $\phi(n) = |U(\mathbb{Z}_n)|$.

Θα δείξουμε ότι $\phi(mn) = \phi(m)\phi(n)$.

Επειδή $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, έχουμε

$$\begin{aligned} |U(\mathbb{Z}_{mn})| &= |U(\mathbb{Z}_m \times \mathbb{Z}_n)| \\ &= |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| \\ &= |U(\mathbb{Z}_m)| |U(\mathbb{Z}_n)|. \end{aligned}$$

Άρα $\phi(mn) = \phi(m)\phi(n)$.

Παρατήρηση. Δεύτερος τρόπος για να δείξουμε στο (2) ότι η φ είναι επί.

Έστω $([a]_m, [b]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Εφόσον $(m, n) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ ώστε $xm + yn = 1$. Άρα $(a - b)xm + (a - b)yn = a - b$ και επομένως

$$a - (a - b)xm = b + (a - b)yn.$$

Έστω $\gamma = a - (a - b)xm = b + (a - b)yn$.

Τότε $a - \gamma = (a - b)xm$, άρα $m \mid a - \gamma$ και επομένως $[a]_m = [\gamma]_m$.

Επίσης $\gamma - b = (a - b)yn$, άρα $n \mid \gamma - b$ και επομένως $[b]_n = [\gamma]_n$.

Οπότε $\varphi([\gamma]_{mn}) = ([\gamma]_m, [\gamma]_n) = ([a]_m, [b]_n)$.

Άρα η φ είναι επί.