Ορισμός: Ένας δακτύλιος R καλείται περιοχή ή δακτύλιος χωρίς διαιρέτες του μηδενός αν $\forall r,s \in R \quad rs=0 \Rightarrow r=0 \text{ ή } s=0$

Δηλαδή ο R είναι περιοχή αν δεν έχει δεξιούς ή αριστερούς διαιρέτες του μηδενός.

. Αν ο δακτύλιος R είναι μεταθετικός με μονάδα και επιπλέον είναι περιοχή, τότε λέγεται ακέραια περιοχή.

Παραδείγματα

1. Ο μεταθετικός δακτύλιος $(\mathbb{Z}_4, +, \cdot)$ δεν είναι ακέραια περιοχή διότι $[2]_4 \neq [0]_4$ και $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$.

Πιο γενικά, έστω n σύνθετος φυσικός αριθμός και έστω ο μεταθετικός δακτύλιος $(\mathbb{Z}_n, +, \cdot)$. Αφού n σύνθετος, γράφουμε $n = mk$, όπου $1 < m, k < n$. Τότε $[m]_n \neq [0]_n$ (διότι αν $[m]_n = [0]_n$ τότε $n \mid m \Rightarrow n \leq m$, άτοπο) και $[m]_n \cdot [k]_n = [mk]_n = [n]_n = [0]_n$, δηλαδή τα στοιχεία $[m]_n$ και $[k]_n$ είναι διαιρέτες του μηδενός.

Συμπέρασμα n σύνθετος $\Rightarrow \mathbb{Z}_n$ όχι ακέραια περιοχή

2. Έστω R προσεταιριστικός δακτύλιος με μονάδα $1 = 1_R$ και έστω $n \in \mathbb{N}$. Για κάθε $i, j = 1, \dots, n$ ορίζεται ο πίνακας

$$E_{ij} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & & 1 & 0 \\ & & 0 & \end{bmatrix} \in M_n(R)$$

θέση (i, j)

Ο $M_n(R)$ δεν είναι περιοχή διότι περιέχει πάντα διαιρέτες του μηδενός. Πράγματι, για $i, j, k, \lambda \in \{1, \dots, n\}$ με $k \neq j$ ισχύει

$$E_{ij} E_{k\lambda} = 0.$$

3. Σε αντίθεση με τα 1. και 2. οι μεταθετικοί δακτύλιοι $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ δεν περιέχαν διαιρέτες του μηδενός και άρα είναι ακέραιες περιοχές.

4. Κάθε υποδακτύλιος μιας (ακέραιας) περιοχής είναι (ακέραια) περιοχή.

5. (SOS, προσοχή) Το ευθύ γινόμενο δύο δακτυλίων R, S με μοναδες 1_R και 1_S αντίστοιχα, δεν είναι ποτέ (ακέραιαι) περιοχή διότι τα στοιχεία $(1_R, 0_S) \in R \times S$ και $(0_R, 1_S) \in R \times S$ είναι διαιρέτες του μηδενός αφού $(1_R, 0_S) \cdot (0_R, 1_S) = (1_R \cdot 0_R, 0_S \cdot 1_S)$
$= (0_R, 0_S) = 0_{R \times S}$

Λήμμα (Νόμοι Διαγραφής): Έστω R μιοι περιοχή. Για κάθε $a, b, c \in R$ ισχύουν:

(i) $a \neq 0, ab = ac \Rightarrow b = c$

(ii) $c \neq 0, ac = bc \Rightarrow a = b$

Αντίστροφα, αν σε κάθε δακτύλιο R ισχύουν οι παραπάνω νόμοι διαγραφής τότε ο R είναι περιοχή.

Απόδειξη: Υποθέτουμε αρχικά ότι ο R είναι περιοχή και θα αποδείξουμε τους νόμους διαγραφής. Έστω $a \neq 0$ και $ab = ac$.

Τότε $ab - ac = 0 \Rightarrow a(b-c) = 0 \xrightarrow[a \neq 0]{R:\text{περιοχή}}$

$b - c = 0 \Rightarrow b = c$.

Αναλόγως, αν $c \neq 0$ και $ac = bc$, τότε θα έχουμε $a = b$. Αντίστροφα, υποθέτουμε ότι σε ένα δακτύλιο R (προσεταιριστικό με μονάδα) ισχύουν οι νόμοι διαγραφής (i) και (ii). Θα αποδείξουμε ότι ο R είναι περιοχή. Πράγματι, έστω $r, s \in R$ με $rs = 0$. Αν $r \neq 0$ θα δείξουμε ότι αναγκαστικά $s = 0$. Πράγματι, $rs = 0$

$\Rightarrow rs = r \cdot 0 \xrightarrow{(i)} s = 0$. Παρόμοια, αν $s \neq 0$ και $rs = 0$ τότε αναγκαστικά $r = 0$.

■

Ορισμός: Ένα στοιχείο $r \in R$ λέγεται **αντιστρέψιμο** αν υπάρχει $s \in R$ έτσι ώστε

$$rs = 1_R = sr.$$

Λήμμα: Κάθε στοιχείο $r \in R$ έχει το πολύ ένα "αντίστροφο" στοιχείο.

Απόδειξη: Έστω $r \in R$. Υποθέτουμε ότι υπάρχουν $s_1, s_2 \in R$ ώστε

$$rs_1 = 1_R = s_1 r \quad (\alpha)$$
$$rs_2 = 1_R = s_2 r \quad (\beta)$$

και θα αποδείξουμε ότι: $s_1 = s_2$.

Πράγματι,

$$s_1 = s_1 \cdot 1_R \overset{(\beta)}{=} s_1 (rs_2)$$
$$= (s_1 \cdot r) s_2$$
$$\underset{=}{(\alpha)} 1_R \cdot s_2$$
$$= s_2. \quad \blacksquare$$

Ορισμός Αν το $r \in R$ είναι αντιστρέψιμο, τότε το μοναδικό $s \in R$ για το οποίο $rs = 1_R = sr$ το συμβολίζουμε με $s = r^{-1}$ και το καλούμε **αντίστροφο** του r.

▼ Το σύνολο όλων των αντιστρέψιμων στοιχείων ενός προσεταιριστικού δακτυλίου R με μονάδα 1_R συμβολίζεται με

$$U(R) := \{r \in R \mid r \text{ αντιστρέψιμο}\} \subseteq R.$$

Πρόταση: Το σύνολο $U(R)$ εφοδιασμένο με την πράξη . του δακτυλίου R είναι ομάδα και καλείται η ομάδα των αντιστρέψιμων στοιχείων του R

Απόδειξη: Επειδή $1_R 1_R = 1_R = 1_R \cdot 1_R$ έπεται ότι 1_R αντιστρέψιμο, άρα $1_R \in U(R)$.

Έστω $r, t \in U(R)$ και θα αποδείξουμε ότι $rt \in U(R)$ και $r^{-1} \in U(R)$.

- $r \in U(R) \Rightarrow \exists s \in R \quad rs = 1_R = sr$ (1)
- $t \in U(R) \Rightarrow \exists v \in R: \quad tv = 1_R = vt$ (2)

Από την (1) έπεται s αντιστρέψιμο και $s = r^{-1} \in U(R)$

Επιπλέον για το στοιχείο $v \in R$ έχουμε

$$rtvs = r \cdot 1_R s = rs = 1_R$$
$$vsrt = v \cdot 1_R t = vt = 1_R$$

Άρα rt αντιστρέψιμο, δηλαδή $rt \in U(R)$ με $(rt)^{-1} = vs = t^{-1} r^{-1}$

Τέλος, επειδή $U(R) \subseteq R$ και η πράξη $\cdot$ είναι προσεταιριστική στο R έπεται ότι η $\cdot$ είναι προσεταιριστική και στο $U(R)$.

Όστε, το ζεύγος $(U(R), \cdot)$ είναι ομάδα με ουδέτερο στοιχείο το 1_R και για κάθε $r \in U(R)$ ο αντίστροφος του r είναι ο r^{-1}. Μάλιστα:

$$\forall r, s \in U(R) \quad (r^{-1})^{-1} = r, \quad (rs)^{-1} = s^{-1} r^{-1}$$

Σημείωση. $0_R \notin U(R)$, άρα $U(R) \subseteq R \setminus \{0\} = R^*$.

Παραδείγματα

(1) Έστω $x \in U(\mathbb{Z})$. Τότε υπάρχει $y \in \mathbb{Z}$ με $xy = 1 = yx$. Άρα, $|xy| = 1 \Rightarrow$

$\Rightarrow |x||y| = 1 \xrightarrow[|y| \in \mathbb{N}]{|x| \in \mathbb{N}} |x| = 1$ ή $|y| = 1$

$\Rightarrow x = \pm 1$ ή $y = \pm 1$. Απ' την άλλη, τα $1, -1$ είναι αντιστρέψιμα με $1^{-1} = 1$, $(-1)^{-1} = -1$

άρα: $U(\mathbb{Z}) = \{-1, 1\}$. (βλέπε Σχόλιο πίσω)

(2) Προφανώς, $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$

(3) Εξ' ορισμού, $\forall n \in \mathbb{N}$, $U(M_n(\mathbb{K})) = GL(n, \mathbb{K})$, όπου $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

(4) Υπενθυμίζουμε ότι για κάθε $n \in \mathbb{N}$

$$U(\mathbb{Z}_n) = \{[k]_n \in \mathbb{Z}_n \mid 1 \leq k \leq n-1, (k, n) = 1\}$$

με $|U(\mathbb{Z}_n)| = \varphi(n)$

↳ η συνάρτηση του Euler.

Σχόλιο: Για $z = x+yi \in \mathbb{C}$ ορίζουμε

$\bar{z} = x-yi \in \mathbb{C}$ και $|z| = \sqrt{x^2+y^2}$.

Ισχύουν οι εξής ιδιότητες: $\forall z, w \in \mathbb{C}$:

$\overline{z \pm w} = \bar{z} \pm \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$, $(\bar{z}) = z$

και τέλος $z\bar{z} = |z|^2$. Προαιρετικά, ας αποδείξουμε την $z\bar{z} = |z|^2$. Αν $z = x+yi$ τότε $z\bar{z} = (x+yi)(x-yi) = x^2 - xyi + yxi - y^2 i^2$

$= x^2 + y^2 = |z|^2$. (άρα $z\bar{z} = |z|^2 \in \mathbb{R}^+$).

Έστω τώρα $z = x+yi \in \mathbb{C}^*$, οπότε $x \neq 0$ ή $y \neq 0$ και συνεπώς $|z|^2 = x^2+y^2 > 0$.

Επειδή $z\bar{z} = |z|^2$ έχουμε: $z \dfrac{\bar{z}}{|z|^2} = 1$

και επειδή ο $\mathbb{C}$ είναι μεταθετικός

ισχύει και $\dfrac{\bar{z}}{|z|^2} z = 1$.

Επομένως, z αντιστρέψιμο, δηλαδή $z \in U(\mathbb{C})$

και μάλιστα $z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{x-yi}{x^2+y^2}$

$$= \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2} i$$

(5) Για τον δακτύλιο $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$

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

Πράγματι, αρχικά: $1 = 1+0i \in \mathbb{Z}[i]$

$-1 = -1+0i \in \mathbb{Z}[i]$

$i = 0+1i \in \mathbb{Z}[i]$

$-i = 0-1i \in \mathbb{Z}[i]$

και $1 \cdot 1 = 1 = 1 \cdot 1$, $(-1)\cdot(-1) = 1 = (-1)(-1)$,

$i \cdot (-i) = -i^2 = 1 = (-i)\cdot i$. Άρα, $1, -1, i, -i \in$

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

Αντίστροφα, έστω $a+bi \in U(\mathbb{Z}[i])$. Τότε

υπάρχει $c+di \in U(\mathbb{Z}[i])$ ώστε

$(a+bi)(c+di) = 1 = (c+di)(a+bi)$. Από το σχόλιο, $c+di = (a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$

$\Rightarrow c = \frac{a}{a^2+b^2}$ και $d = -\frac{b}{a^2+b^2}$.

$c \in \mathbb{Z} \Rightarrow \frac{a}{a^2+b^2} \in \mathbb{Z} \Rightarrow a^2+b^2 \mid a$.

Άλλα, $a^2+b^2 \geq a^2 \geq a$, εκτός αν:

$a=0$ ή $a=\pm 1$.

Ομοίως βρίσκουμε $b=0$ ή $b=\pm 1$

και άρα: $a+bi \in \{1, -1, i, -i\}$, δηλαδή

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

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

H/W: Να βρεθεί η $U(\mathbb{Q}[i])$, όπου

$\mathbb{Q}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$

Ομοίως, η $U(\mathbb{Q}[\sqrt{2}])$, όπου $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$

(6) Για τον δακτύλιο τετρανίων του Hamilton

$$\mathbb{H} = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in \mathbb{M}_2(\mathbb{C}) \mid a, b \in \mathbb{C} \right\}$$

έχουμε ότι $U(\mathbb{H}) = \mathbb{H} \setminus \{0\} = \mathbb{H}^*$

Απόδειξη: Εξ' ορισμού $U(\mathbb{H}) \subseteq \mathbb{H}^*$. Έστω

τώρα $X = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in \mathbb{H}^*$, οπότε $a \neq 0$ ή $b \neq 0$.

$\det(X) = a\bar{a} + \bar{b}b = |a|^2 + |b|^2 > 0$, άρα ο

X είναι αντιστρέψιμος πίνακας και από

γνωστή διαδικασία της Γραμμικής Άλγεβρας

βρίσκουμε $X^{-1} = \frac{1}{\det(X)} \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} \Longrightarrow$

$$\Longrightarrow X^{-1} = \begin{bmatrix} \frac{\bar{a}}{\det(X)} & -\frac{b}{\det(X)} \\ -\left(\frac{b}{\det(X)}\right) & \left(\frac{\bar{a}}{\det(X)}\right) \end{bmatrix} \in \mathbb{H}.$$

Επειδή $X^{-1} \in \mathbb{H}$ και $XX^{-1} = I_2 = X^{-1}X$

έπεται ότι $X \in U(\mathbb{H})$. Άρα $\mathbb{H}^* \subseteq U(\mathbb{H})$.

Τελικά, $U(\mathbb{H}) = \mathbb{H}^*$. ∎

Ορισμός: ① Ένας προσεταιριστικός δακτύλιος $(R, +, \cdot)$ με μονάδα, λέγεται **δακτύλιος διαίρεσης** αν κάθε μη-μηδενικό στοιχείο του R είναι αντιστρέψιμο, δηλαδή αν $U(R) = R^*$.

② Ένας μεταθετικός δακτύλιος διαίρεσης καλείται **σώμα**.

Παραδείγματα

① Οι δακτύλιοι $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ και $(\mathbb{C}, +, \cdot)$ είναι σώματα διότι είναι μεταθετικοί και επιπλέον $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$.

(2) Ο δακτύλιος $\mathbb{H}$ των τετρανίων του Hamilton δεν είναι μεταθετικός και $U(\mathbb{H}) = \mathbb{H}^*$. Δηλαδή, ο $\mathbb{H}$ είναι δακτύλιος διαίρεσης ο οποίος δεν είναι σώμα.

(3) Θεωρούμε τον μεταθετικό υποδακτύλιο $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ του σώματος $\mathbb{R}$. Έστω $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ με $a+b\sqrt{2} \neq 0$. Τότε $a \neq 0$ ή $b \neq 0$. Ισχύει ότι:

$$(a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 \quad (*)$$

Διακρίνουμε τις εξής περιπτώσεις:

(i) $a = 0, b \neq 0$. Τότε $a^2 - 2b^2 = -2b^2 \neq 0$

(ii) $a \neq 0, b = 0$. Τότε $a^2 - 2b^2 = a^2 \neq 0$

(iii) $a \neq 0, b \neq 0$. Αν $a^2 - 2b^2 = 0$, τότε

$$a^2 = 2b^2 \to \left(\frac{a}{b}\right)^2 = 2 \Rightarrow \sqrt{2} = \frac{|a|}{|b|} \in \mathbb{Q},$$

άτοπο, άρα: $a^2 - 2b^2 \neq 0$.

Σε κάθε περίπτωση ξέρουν, $a^2-2b^2 \neq 0$ και λόγω (*): $(a+b\sqrt{2})\dfrac{(a-b\sqrt{2})}{a^2-2b^2} = 1$ (**).

Επειδή $\dfrac{a-b\sqrt{2}}{a^2-2b^2} = \dfrac{a}{a^2-2b^2} - \dfrac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

από την τελευταία ισότητα (**) έπεται

$a+b\sqrt{2} \in U(\mathbb{Q}[\sqrt{2}])$ με $(a+b\sqrt{2})^{-1} = \dfrac{a}{a^2-2b^2} - \dfrac{b}{a^2-2b^2}\sqrt{2}$

Συνεπώς, κάθε μη-μηδενικό στοιχείο του $\mathbb{Q}[\sqrt{2}]$ αντιστρέφεται και άρα ο $\mathbb{Q}[\sqrt{2}]$ είναι σώμα.

④ Ο δακτύλιος $\mathbb{Z}$ είναι ακέραια περιοχή αλλά όχι σώμα διότι $U(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z}^*$.

Αντίστοιχα, ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι ακέραια περιοχή (ως υποδακτύλιος του ℂ) αλλά όχι σώμα αφού $U(\mathbb{Z}[i]) = \{-1, 1, i, -i\} \neq \mathbb{Z}[i]^*$

H/W Νδο ο $\mathbb{Q}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$ είναι σώμα.

⑤ Για $n \in \mathbb{N}$, $n \geq 2$ και $(R, +, \cdot)$ προσεταιριστικό δακτύλιο με μονάδα, ο δακτύλιος $(M_n(R), +, \cdot)$ δεν είναι σώμα διότι δεν είναι μεταθετικός. Δεν είναι ούτε δακτύλιος διαίρεσης διότι όπως έχουμε δείξει δεν είναι και περιοχή. (δες επόμενη πρόταση)

Πρόταση R: σώμα $\Longrightarrow$ R: δακτύλιος διαίρεσης $\Longrightarrow$ R: περιοχή

Δεν ισχύουν οι αντίστροφες συνεπαγωγές.

Απόδειξη: Βήμα 1: Εξ' ορισμού, κάθε σώμα είναι δακτύλιος διαίρεσης.

Βήμα 2: Έστω R δακτύλιος διαίρεσης και θα αποδείξουμε ότι R: περιοχή.

Έστω λοιπόν $r, s \in R$ με $rs = 0_R$ και θα αποδείξουμε ότι $r = 0_R$ ή $s = 0_R$.

Αν $r \neq 0_R$ τότε επειδή ο R είναι δακτύλιος διαίρεσης, υπάρχει το $r^{-1} \in R$ με $rr^{-1} = 1_R = r^{-1}r$. Τότε $rs = 0_R \Rightarrow$

$r^{-1}(rs) = r^{-1} \cdot 0_R \Rightarrow (r^{-1}r)s = 0_R \Rightarrow 1_R \cdot s = 0_R$

$\Rightarrow s = 0_R$.

Βήμα 3: R: δακτύλιος διαίρεσης $\not\Rightarrow$ R: σώμα

Αντιπαράδειγμα $R = \mathbb{H}$.

Βήμα 4 R: περιοχή $\not\Rightarrow$ R δακτύλιος διαίρεσης

Αντιπαράδειγμα: $R = \mathbb{Z}$. ∎

Οι αντίστροφες συνεπαγωγές είναι αληθείς αν περιοριστούμε στην κλάση των πεπερασμένων δακτυλίων.

Θεώρημα Wedderburn (1905) (Χωρίς απόδειξη)

Κάθε δακτύλιος διαίρεσης με πεπερασμένο πλήθος στοιχείων είναι μεταθετικός και άρα είναι σώμα.

Θεώρημα (SOS) Κάθε περιοχή με πεπερασμένο πλήθος στοιχείων είναι δακτύλιος διαίρεσης.

Ιδιαίτερα, κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη: Έστω R μια πεπερασμένη περιοχή και έστω $R = \{r_1, r_2, \ldots, r_n\}$.

Έστω $x \in R$, $x \neq 0_R$ και ορίζουμε απεικόνιση $f_x : R \to R$ με $f_x(r) = xr$.

- f_x: 1-1 στο R: Έστω $f_x(r) = f_x(s)$ και θα αποδείξουμε ότι $r = s$.

Πράγματι, $f_x(r) = f_x(s) \Rightarrow xr = xs$

$\Rightarrow x(r-s) = 0_R \xrightarrow[\text{περιοχή } x \neq 0_R]{R:} r-s = 0_R \Rightarrow r = s.$

Εφόσον $|R| < \infty$ και η f_x είναι 1-1 έπεται ότι f_x: επί του R. Άρα, για το $1_R \in R$ υπάρχει $r_j \in R$ με $f_x(r_j) = 1_R$. δηλαδή: $xr_j = 1_R$ (1). Εργαζόμενοι ακριβώς ανάλογα με την απεικόνιση $g_x: R \to R$ με $g_x(r) = rx$, βλέπουμε ότι g_x: 1-1 και επί, οπότε για το $1_R \in R$ υπάρχει $r_i \in R$ με $g_x(r_i) = 1_R \Rightarrow r_i x = 1_R$ (2).

Τότε: $r_j = 1_R \cdot r_j \overset{(2)}{=} (r_i x) r_j = r_i (x r_j)$

$\overset{(1)}{=} r_i 1_R = r_i$

οπότε: $xr_i = 1_R = r_i x$, γεγονός που δηλώνει ότι το x είναι αντιστρέψιμο.

Έτσι, κάθε μη-μηδενικό στοιχείο του R είναι αντιστρέψιμο και επομένως ο R είναι δακτύλιος διαίρεσης.

Ιδιαίτερα, αν ο R είναι πεπερασμένη ακέραια περιοχή τότε R: μεταθετικός δακτύλιος διαίρεσης, άρα R: σώμα. ∎

ΠΕΡΙΛΗΨΗ

ΓΕΝΙΚΑ Για οποιονδήποτε δακτύλιο R ισχύουν τα εξής

R: σώμα $\Longrightarrow$ R: δακτύλιος διαίρεσης $\Longrightarrow$ R: περιοχή

$\not\Longleftarrow$ $(R = \mathbb{H})$ $\not\Longleftarrow$ $(R = \mathbb{Z})$

• Αν όμως R: δακτύλιος με $|R| < \infty$, τότε:

R: σώμα $\Longleftrightarrow$ R: δακτύλιος διαίρεσης $\Longleftrightarrow$ R: ακέραιη περιοχή

Πρόταση (SOS) Έστω $n \in \mathbb{N}$, $n \geq 2$. Για τον δακτύλιο $(\mathbb{Z}_n, +, \cdot)$ τα ακόλουθα ισοδυναμούν:

(i) Ο $\mathbb{Z}_n$ είναι σώμα

(ii) Ο $\mathbb{Z}_n$ είναι ακέραια περιοχή

(iii) n: πρώτος αριθμός

Απόδειξη

(i) $\Rightarrow$ (ii) Κάθε σώμα είναι ακέραια περιοχή

(ii) $\Rightarrow$ (iii) Έχουμε δείξει στη θεωρία ότι αν n: σύνθετος τότε $\mathbb{Z}_n$ όχι ακέραια περιοχή, άρα $\mathbb{Z}_n$ ακέραια περιοχή $\Rightarrow$ n: πρώτος.

(iii) $\Rightarrow$ (i) Έστω $n = p$: πρώτος και θα δείξουμε $\mathbb{Z}_p$: σώμα. Επειδή $\mathbb{Z}_p$: μεταθετικός, αρκεί να δείξουμε ότι κάθε μη-μηδενικό στοιχείο του ότι είναι αντιστρέψιμο. Έστω $[k]_p \in \mathbb{Z}_p$ με $[k]_p \neq [0]_p$. Τότε $p \nmid k$ και επειδή p: πρώτος, ισχύει $(k, p) = 1$.

Επομένως, υπάρχουν $x, y \in \mathbb{Z}$ ώστε

$kx + py = 1$, άρα: $[kx+py]_p = [1]_p \Rightarrow$

$\Rightarrow [kx]_p + [py]_p = [1]_p \Rightarrow [k]_p[x]_p + \underbrace{[p]_p}_{[0]_p}[y]_p = [1]_p$

$\Rightarrow [k]_p[x]_p = [1]_p = [x]_p[k]_p$,

όπότε $[k]_p \in U(\mathbb{Z}_p)$, όπως θέλαμε. ∎

2η απόδειξη για τη συνεπαγωγή (iii) $\Rightarrow$ (i)

Αν p πρώτος, τότε $\varphi(p) = p-1$, άρα:

$U(\mathbb{Z}_p) = \{[1]_p, [2]_p, \ldots, [p-1]_p\} = \mathbb{Z}_p^*$

3η απόδειξη για τη συνεπαγωγή (iii) $\Rightarrow$ (i)

$n = p$ πρώτος ο $\mathbb{Z}_p$ είναι μεταθετικός με $|\mathbb{Z}_p| = p < \infty$ και άρα αρκεί να δείξουμε ότι ο $\mathbb{Z}_p$ είναι περιοχή. Προς τούτο, έστω $[k]_p, [\lambda]_p \in \mathbb{Z}_p$ με $[k]_p[\lambda]_p = [0]_p$.

$$\Rightarrow [k\lambda]_p = [0]_p \Rightarrow p \mid k\lambda$$

$$\xRightarrow{P:\ \text{πρώτος}} p \mid k \text{ ή } p \mid \lambda$$

$$\Rightarrow [k]_p = [0]_p \text{ ή } [\lambda]_p = [0]_p.$$

■