

Previously on Beligiannis

R : Δακτύλιος με μονάδα $1 = 1_R$, τότε:

$$U(R) = \{r \in R \mid r: \text{αντιστρέψιμο}\} = \{r \in R \mid \exists s \in R: s \cdot r = 1_R = r \cdot s\}$$

Το $s \in R: s \cdot r = 1_R$ είναι μοναδικό και καλείται αντιστροφή του r και το συμβολίζεται με $s = r^{-1}$

Το ζεύγος $(U(R), \cdot)$ αποτελεί ομάδα

Παράδειγμα: ① $U(\mathbb{Z}) = \{1, -1\}$

② Αν $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, τότε: $U(K) = K^* = K - \{0\}$

Αν $S \subseteq R$, τότε: S υποδακτύλιος του $R \iff$

① $0 \in S$, ② $\forall x, y \in S: x - y \in S$, ③ $\forall x, y \in S: x \cdot y \in S$

Κάθε υποδακτύλιος ενός δακτύλιου είναι υποδακτύλιος με τις επαχόμενες πράξεις.

③ $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

Προφανώς $\mathbb{Z}[i]$ είναι υποδακτύλιος του $\mathbb{C}$ κι άρα είναι δακτύλιος.

Ο $\mathbb{Z}[i]$ καλείται ο δακτύλιος των ακεραίων του Gauss.

Θα προσδιορίσουμε την ομάδα $U(\mathbb{Z}[i])$

Έστω $a+bi \in U(\mathbb{Z}[i]) \Rightarrow \exists c+di \in \mathbb{Z}[i]$

$$(a+bi)(c+di)=1 \Rightarrow (ac-bd) + (ad+bc)i=1$$

$$\Rightarrow \begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases} \Rightarrow c = \frac{a}{a^2+b^2} \quad d = \frac{-b}{a^2+b^2}, \quad a, b \neq 0$$

$a^2+b^2 = n > 0$. Τότε επειδή: $a = c \cdot n$ και $b = -d \cdot n$

$$\Rightarrow n|a \text{ και } n|b$$

$$n = a^2 + b^2 = (cn)^2 + (-dn)^2 = n^2 c^2 + n^2 d^2 = n^2(c^2 + d^2)$$

$$\Rightarrow n(c^2 + d^2) = 1 \Rightarrow \underline{n=1}$$

$$\text{Άρα, } a^2 + b^2 = 1 \Rightarrow \begin{cases} a^2=1 \\ b^2=0 \end{cases} \quad \text{ή} \quad \begin{cases} a^2=0 \\ b^2=1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a=\pm 1 \\ b=0 \end{cases} \quad \text{ή} \quad \begin{cases} a=0 \\ b=\pm 1 \end{cases}$$

$$\Rightarrow \begin{cases} a=\pm 1 \\ b=0 \end{cases} \quad \text{ή} \quad \begin{cases} a=0 \\ b=\pm 1 \end{cases} \Rightarrow a+bi = 1 \text{ ή } -1 \text{ ή } i \text{ ή } -i$$

$$\text{Άρα, } U(\mathbb{Z}[i]) = \{1, -1, i, -i\} = \langle i \rangle = U_4$$

④ Z_n : Ο δακτύλιος των ακεραίων modulo n :

$$U(Z_n) = \{ [k]_n \in Z_n \mid (k, n) = 1 \}$$

$$\text{Έστω } [k]_n \in U(Z_n) \Rightarrow \exists [m]_n \in Z_n: [k]_n \cdot [m]_n = [1]_n \Rightarrow$$

$$\Rightarrow [k \cdot m]_n = [1]_n \Rightarrow n \mid 1 - k \cdot m \Rightarrow \exists \lambda \in \mathbb{Z}: 1 - km = n \cdot \lambda$$

$$\Rightarrow km + n\lambda = 1 \Rightarrow (k, n) = 1$$

$$\text{Αντίστροφα, αν } (k, n) = 1 \Rightarrow \exists m, \lambda \in \mathbb{Z}: k \cdot m + n \cdot \lambda = 1$$

$$\Rightarrow [k \cdot m + n \cdot \lambda]_n = [1]_n \Rightarrow [k]_n [m]_n + \underbrace{[n]_n [\lambda]_n}_0 = [1]_n$$

$$\Rightarrow [k]_n \cdot [m]_n = [1]_n \Rightarrow [m]_n \cdot [k]_n = [1]_n$$

$$\Rightarrow [k]_n \in U(Z_n)$$

$$\leadsto \text{Αν } p: \text{πρώτος, τότε } U(Z_p) = Z_p^* = Z_p - \{[0]_p\}$$

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

Ορισμός: Ένας δακτύλιος με μονάδα 1 καλείται δακτύλιος διαίρεσης αν-ν

$U(R) = R^*$, δηλαδή: κάθε μη-μηδενικό στοιχείο του είναι αντιστρέψιμο

Ορισμός: Ένας μεταθετικός δακτύλιος διαίρεσης καλείται σώμα.

Παράδειγμα: Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα

Ο δακτύλιος $\mathbb{Z}$ δεν είναι σώμα.

Πρόταση: Ο δακτύλιος $\mathbb{Z}_n$ θα είναι σώμα μόνο όταν το n : πρώτος (και αντιστρόφως)

Απόδειξη: $\mathbb{Z}_n$: σώμα $\Leftrightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n^* \Leftrightarrow$

$\Leftrightarrow [k]_n \in \{[1]_n, \dots, [n-1]_n\} : (k, n) = 1 \Leftrightarrow n$: πρώτος

Πρόβλημα: Υπάρχουν μη-μεταθετικοί δακτύλιοι διαίρεσης;

Θεωρούμε το δακτύλιο $M_2(\mathbb{C})$

$\left\{ \begin{array}{l} \text{Αν } K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \text{ τότε: } U(M_2(K)) = GL(2, K) = \\ = \{A \in M_2(K) \mid \det A \neq 0\} \end{array} \right\}$

Ο $M_2(\mathbb{C})$ δεν είναι μεταθετικός, ούτε δακτύλιος διαίρεσης.

NO:

Date:

Θα θεωρήσουμε το σύνολο $H = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in M_2(\mathbb{C}) \mid z, w \in \mathbb{C} \right\} \subseteq M_2$

Επειδή $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in H$ και αν $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}, \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \in H$, τότε:

$$\begin{pmatrix} z & \bar{w} \\ -\bar{w} & \bar{z} \end{pmatrix} - \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = \begin{pmatrix} z-u & w-v \\ -(\bar{w}-\bar{v}) & \bar{z}-\bar{u} \end{pmatrix} \in H$$

$$\text{Αν } \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = \begin{pmatrix} zu - w\bar{v} & zv + w\bar{u} \\ -\bar{w}u - \bar{z}\bar{v} & -\bar{w}v + \bar{z}\bar{u} \end{pmatrix} =$$

$$= \begin{pmatrix} zu - w\bar{v} & zv + w\bar{u} \\ -(\overline{zv + w\bar{u}}) & \overline{zu - w\bar{v}} \end{pmatrix} \in H. \text{ Άρα } H \text{ υποδακτύλιος του } M_2(\mathbb{C})$$

Οπότε H είναι δακτύλιος και καλείται δακτύλιος των τετρανίων του Hamilton, ο οποίος δεν είναι μεταθετικός, διότι:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

ΘΣο: Κάθε μη-μηδενικό στοιχείο A του H είναι αντιστρέψιμο

$$\mathbb{0} \neq A = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in H, \quad |A| = z \cdot \bar{z} + w \cdot \bar{w} = |z|^2 + |w|^2.$$

Επειδή $A \neq \mathbb{0}$, προκύπτει πως τα $(z, w) \neq (0, 0)$, οπότε

$$|A| \neq 0 \Rightarrow \mathbb{0} \neq A \text{ είναι αντιστρέψιμο.}$$

$$A^{-1} = \begin{pmatrix} \bar{z}/\Delta & -w/\Delta \\ -\bar{w}/\Delta & z/\Delta \end{pmatrix}, \text{ όπου } \Delta = |z|^2 + |w|^2$$

άρα, $A^{-1} \in H$. Οπότε, ο H είναι $\{n\}$ -μεταθετικός δακτύλιος διαίρεσης.

$$\text{Αν } (x_0, x_1, x_2, x_3)(y_0, y_1, y_2, y_3) = (z_0, z_1, z_2, z_3)$$

$$\begin{pmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -(x_2 - ix_3) & x_0 - ix_1 \end{pmatrix} \begin{pmatrix} y_0 + iy_1 & y_2 + iy_3 \\ -(y_2 - iy_3) & y_0 - iy_1 \end{pmatrix} =$$

$$= \begin{pmatrix} z_0 + iz_1 & z_2 + iz_3 \\ -(z_2 - iz_3) & z_0 - iz_1 \end{pmatrix}$$

Παρατήρηση: Σώφα $\Rightarrow$ Δακτύλιος Διαίρεσης

Το παράδειγμα των τετρανίων του Hamilton, δείχνει ότι η παραπάνω συνεπαχυσή δεν αντιστρέφεται.

Θεώρημα (Wedderburn - 1905): Κάθε πεπερασμένος δακτύλιος διαίρεσης είναι σώφα.

Θεώρημα (Jacobson - 1935): Έστω R : δακτύλιος

για τον οποίο ισχύει ότι: $\forall x \in R : \exists n = n_x \in \mathbb{N} :$

$x^n = x$. Τότε, ο δακτύλιος R είναι μεταθετικός

NO:

Date:

Πρόταση: Θεώρημα Jacobson $\Rightarrow$ Θεώρημα Wedderburn

Έστω R : πεπερασμένος δακτύλιος διαίρεσης $\Rightarrow |R| = n$

Τότε: $R^* = U(R)$, τάξης $n-1$

Από το Θ. Lagrange $\Rightarrow \forall x \in R^*: x^{n-1} = 1_R \Rightarrow$

$\Rightarrow \underline{x^n = x}$. Από Θ. Jacobson $\Rightarrow R$: μεταθετικός

Ορισμός: Έστω R : δακτύλιος. Ένα στοιχείο $\alpha \in R^*$ καλείται αριστερός διαυρέτης του 0 αν $\alpha v = 0$

$\exists b \in R^*: \alpha \cdot b = 0$. Παρόμοια ορίζεται η έννοια του δεξιού διαυρέτη του μηδενός.

Ορισμός: Ένας μεταθετικός δακτύλιος με $1 \neq 0$ χωρίς διαυρέτες του μηδενός, καλείται ακέραια περιοχή.

Παραδείγματα: ① Δακτύλιος διαίρεσης $\Rightarrow$ Δεν υπάρχουν δεξιοί ή αριστεροί διαυρέτες του μηδενός

② Κάθε σώμα είναι ακέραια περιοχή

Για το ①: Έστω R : δακτύλιος διαίρεσης κι έστω α : αριστερός διαυρέτης του μηδενός στο R

$\Rightarrow \alpha \in R^*$ και $\exists b \in R^*: \alpha \cdot b = 0 \Rightarrow \alpha' \cdot \alpha \cdot b = 0 \Rightarrow$
 $\Rightarrow 1 \cdot b = 0 \Rightarrow$
 $\Rightarrow b = 0$: ΑΤΟΝΟ

$\hookrightarrow \exists \alpha' \in R: \alpha' \cdot \alpha = 1_R$

NO:

Date:

Το ② προκύπτει άμεσα απ' το ①

Παρατήρηση: Υπάρχουν ακέραες περιοχές που δεν είναι σώματα

Θεώρημα: Κάθε πεπερασμένη ακέραα περιοχή είναι σώμα.

Απόδειξη: Έστω R : ακέραα περιοχή και $|R| < \infty$

Θδο: R είναι σώμα

Ανταδύ, 9δο: κάθε μη-μηδενικό στοιχείο $x \in R$ είναι αντιστρέψιμο

Ορίσαμε απεικόνιση $f_x: R \rightarrow R$, $f_x(r) = r \cdot x$

Η $f_x: I-I$, διότι $f_x(r) = f_x(s) \Rightarrow r \cdot x = s \cdot x \Rightarrow r \cdot x - s \cdot x = 0$

$\Rightarrow (r-s) \cdot x = 0$, επειδή $x \neq 0$ κι επειδή R : ακέραα περιοχή

$\Rightarrow r-s=0 \Rightarrow \underline{r=s}$

Οπότε $f_x: I-I$. Επειδή $|R| < \infty$, η f_x είναι επι

$\Rightarrow$ για το $1_R: \exists y \in R: f_x(y) = 1_R \Rightarrow y \cdot x = 1_R$
επειδή R : μεταθετικός

$\Rightarrow x \cdot y = 1_R$ Οπότε x : αντιστρέψιμο

Άρα, ο δακτύλιος R είναι σώμα

• Κάθε πεπερασμένος δακτύλιος διαίρεσης δεν έχει διαυρέτες του μηδενός

Πρόταση: Το στοιχείο $[k]_n \in \mathbb{Z}_n$ είναι διαυρέτης του 0 $\Leftrightarrow$
 $\Leftrightarrow (k, n) > 1$

Απόδειξη: " $\Rightarrow$ " Έστω ότι $[k]_n$ είναι διαυρέτης του μηδενός

$\Rightarrow [k]_n \neq [0]_n$ και υπάρχει $[l]_n \neq 0 : [k]_n \cdot [l]_n = [0]_n$

Αν $(k, n) = 1 \Rightarrow [k]_n$ αντιστρέφεται $\Rightarrow$

$\Rightarrow \exists [m]_n \in \mathbb{Z}_n : [m]_n [k]_n = [1]_n \Rightarrow$

$\Rightarrow [m]_n [k]_n [l]_n = [0]_n \Rightarrow [l]_n = [0]_n$: Άτοπο

" $\Leftarrow$ " Έστω $(k, n) = d > 1$. Τότε: $d|n$ και $d|k$, άρα:

$$\frac{k}{d}, \frac{n}{d} \in \mathbb{Z}. \text{ Τότε: } [k]_n \left[\frac{n}{d} \right]_n = \left[\frac{k \cdot n}{d} \right]_n = \left[\frac{k}{d} \cdot n \right]_n \\ = \left[\frac{k}{d} \right]_n [n]_n = [0]_n$$

Όπως, αν $\left[\frac{n}{d} \right]_n = [0]_n \Rightarrow n | \frac{n}{d} \Rightarrow n \leq \frac{n}{d}$: άτοπο

διότι $d > 1$. Παρόμοια $[k]_n \neq [0]_n$

Άρα, $[k]_n$: διαυρέτης του μηδενός

Πρόταση: Ο δακτύλιος $\mathbb{Z}_n$: αθέρα περιοχή $\Leftrightarrow n$: πρώτος

NO:

Date:

Απόδειξη: Ο $\mathbb{Z}_n$ είναι ακέραια περιοχή $(\Leftrightarrow)$

$(\Leftrightarrow)$ Ο $\mathbb{Z}_n$ δεν έχει διαφύκτες του μηδενός $(\Leftrightarrow)$

$(\Leftrightarrow) \nexists [k]_n \in \mathbb{Z}_n : (k,n)=1 \Leftrightarrow n = \text{πρώτος}$
($[k]_n \neq 0$)

Θεώρημα: Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα $(\Leftrightarrow)$

$(\Leftrightarrow) \mathbb{Z}_n$: ακέραια περιοχή $(\Leftrightarrow) n$: πρώτος

Η εξίσωση $x^2 - 5x + 6 = 0$ έχει 2 ρίζες, τις $-2, -3$
στο $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Στο $\mathbb{Z}_{12}$ η εξίσωση έχει περισσότερες ρίζες

Έστω $\mathbb{R}$: μη-μεταθετικός δακτύλιος $\Rightarrow$

$\Rightarrow \exists x, y \in \mathbb{R} : xy \neq yx$

Στο δακτύλιο $M_2(\mathbb{R})$ έστω ο πίνακας

$A = \begin{pmatrix} x & y \\ x & y \end{pmatrix}, |A| = xy - yx \neq 0$

Έστω $\mathbb{R}_1, \mathbb{R}_2$: δακτύλιοι με μονάδα

NO:

Date:

$R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$. Ορίζουμε πράξεις

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

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

Η τριάδα $(R_1 \times R_2, +, \cdot)$: δακτύλιος με μονάδα

$$1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$$

Ο $R_1 \times R_2$: έχει πάντα διαμέριτες του 0, άρα δεν είναι ποτέ σώμα ή αθέριμα περιοχή, διότι:

$$(1_{R_1}, 0)(0, 1_{R_2}) = (0, 0)$$

$$U(R_1 \times R_2) = U(R_1) \times U(R_2)$$

R : μεταθετικός δακτύλιος με μονάδα

$$R[[t]] = \{(a_n)_{n \geq 0} = \sum_{k=0}^{\infty} a_k t^k \mid a_k \in R, \forall k \geq 0\}$$

$$R[t] = \{(a_n)_{n \geq 0} = \sum_{k=0}^{\infty} a_k t^k \mid \exists n \in \mathbb{N}: a_k = 0, \forall k > n\}$$

$R[t]$: υποδακτύλιος του $R[[t]]$, διότι: $0 \in R[t] \in R[t]$, αν

$$P(t) = a_0 + a_1 t + \dots + a_n t^n, Q(t) = b_0 + b_1 t + \dots + b_m t^m$$

είναι στοιχεία του $R[t]$, τότε $P(t) - Q(t) \in R[t]$,

$P(t) \cdot Q(t) \in R[t]$. Άρα $R[t]$: δακτύλιος με μονάδα.

Υποθέτουμε ότι: R αρέσμαια περιοχή

Έστω $P(t) = a_0 + a_1 t + \dots + a_n t^n \in R[t]$

① Αν $a_i = 0 \ \forall i \geq 0$, τότε $P(t) = 0$: μηδενικό στοιχείο
Σακουλίου

② Αν $a_i = 0 \ \forall i \geq 1$ και $a_0 \neq 0$, τότε $P(t) = a_0 =$

$= a_0 \cdot 1_{R[t]} = (a_0, 0, 0, \dots, 0)$, είναι ένα σταθερό μη-μηδενικό πολυώνυμο και ορίζουμε το βαθμό του,
 $\deg P(t) = 0$

③ Αν $\exists i \geq 1 : a_i \neq 0$, τότε ορίζουμε

$$\deg P(t) = \max \{k \in \mathbb{N} \mid a_k \neq 0\}$$

Έστω $P(t), Q(t)$ δύο μη-μηδενικά πολυώνυμα

$$\bullet \deg(P(t) + Q(t)) \leq \max \{\deg P(t), \deg Q(t)\} \\ \text{αν } P(t) + Q(t) \neq 0$$

$$\left. \begin{array}{l} P(t) = a_0 + a_1 t + \dots + a_n t^n, \deg P(t) = n \\ Q(t) = b_0 + b_1 t + \dots + b_m t^m, \deg(Q(t)) = m \end{array} \right\} \Rightarrow$$

$$\begin{array}{l} a_n \neq 0 \implies a_n b_m \neq 0 \implies \deg(P(t)Q(t)) = n+m \\ b_m \neq 0 \end{array} \quad R: \text{αρέσμαια} \\ \text{περιοχή}$$

Ο Σακτούλιος R : αθέραμα περιοχή $\Rightarrow$ ο Σακτούλιος των ποινωμένων $R[t]$: αθέραμα περιοχή, διότι:

$$\text{Av } P(t) - Q(t) = 0, \text{ τότε } P(t) = 0 \text{ ή } Q(t) = 0$$

Η απόδειξη είναι όπως και πριν:

$$\text{Av } P(t) \neq 0 \text{ και } Q(t) \neq 0$$

$$\deg P(t) = n \quad \deg (P(t)Q(t)) = n+m \Rightarrow$$

$$\deg Q(t) = m \quad \Rightarrow P(t)Q(t) \neq 0 : \underline{\text{άτονο}}$$

Ο $R[t]$ δεν έχει διαμέτες του μηδενός

Άρα είναι αθέραμα περιοχή

$$\text{Στο } \mathbb{Z}_6 : \left. \begin{array}{l} P(t) = [2]_6 \neq [0]_6 \\ Q(t) = [3]_6 \neq [0]_6 \end{array} \right\} \Rightarrow P(t)Q(t) = [6]_6 = [0]_6$$