21/5/2018

ΑΝΑΠΛΗΡΩΣΕΙΣ: Παρασκευή 25/5 15.00 - 19.00
Τετάρτη 30/5 14.00 - 16.00

ΟΡΙΣΜΟΣ Έστω $R$ δακτύλιος και $S \subseteq R$. Το $S$ λέγεται ΥΠΟΔΑΚΤΥΛΙΟΣ του $R$ αν
i) $(S,+)$ υποομάδα του $(R,+)$ (άρα $0_R = 0_S \in S$)
ii) Αν $a,b \in S$ τότε $a \cdot b \in S$

ΠΡΟΣΟΧΗ Άλλο υποδακτύλιος, άλλο ιδεώδες!

ΠΑΡΑΤΗΡΗΣΗ Αν $S$ υποδακτύλιος του $R$, τότε $(S,+,\cdot)$ δακτύλιος.

Πρόταση: Αν $S$ ιδεώδες του $R$ τότε $S$ υποδακτύλιος του $R$. Γενικά το αντίστροφο δεν ισχύει.

Απόδειξη Έστω $S$ ιδεώδες του $R$. Από τον ορισμό $S$ υποδακτύλιος του $R$.

Παραδείγμα Έστω $R = \mathbb{Q}$, $S = \mathbb{Z}$. Φανερά $S$ υποδακτύλιος του $R$ (γιατί $(\mathbb{Z},+)$ υποομάδα του $(\mathbb{Q},+)$ και αν $a,b \in \mathbb{Z}$ τότε $a \cdot b \in \mathbb{Z}$)
Αλλά το $S$ ΟΧΙ ιδεώδες του $\mathbb{Q}$, γιατί
$1 \in S$, $\frac{1}{2} \in R$ αλλά $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin S$

(Παρόμοια $\mathbb{Q}$ υποδακτύλιος του $\mathbb{R}$ αλλά όχι ιδεώδες
$\mathbb{Z}$ << << $\mathbb{R}$ << << << κλπ)

ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ ΔΑΚΤΥΛΙΟΥ
Έστω $R$ δακτύλιος. Θέτουμε $A = \{n \in \mathbb{Z}, n \geq 1$ και $n \cdot a = 0_R$ για κάθε $a \in R\}$. Αν $A = \emptyset$ λέμε ότι ο $R$ έχει χαρακτηριστική 0 (μηδέν). Αν $A \neq \emptyset$, λέμε ότι ο $R$ έχει χαρακτηριστική το ΕΛΑΧΙΣΤΟ στοιχείο του $A$.

Παράδειγμα 1) $R = \mathbb{Z}$. Τότε $\mathcal{A} = \emptyset$, διατί $\operatorname{ord}_{(\mathbb{Z},+)} 1_{\mathbb{Z}} = +\infty$

Άρα ο $\mathbb{Z}$ έχει χαρακτηριστική 0. Ομοίως, οι δακτύλιοι $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}^{m\times m}, m \geq 1$ έχουν χαρακτηριστική 0.

2) Έστω $R = \mathbb{Z}_3$. Τότε $\mathcal{A} = \{3, 6, 9, \ldots\}$

$\{[0]_3, [1]_3, [2]_3\}$

Συνεπώς το $\mathbb{Z}_3$ έχει χαρακτηριστική 3.

Πρόταση Έστω $R$ ακέραια περιοχή. Τότε ή η $R$ έχει χαρακτηριστική μηδέν ή έχει χαρακτηριστική $p$, όπου $p$ πρώτος.

(Σαν πόρισμα ΔΕΝ υπάρχει ακέραια περιοχή με χαρακτηριστική 4 ή 6 κλπ.)

Απόδειξη Αφού $R$ ακέραια περιοχή, έχουμε $R$ μεταθ. δακτύλιος με $1_R \neq 0_R$ και $a, b \in R \setminus \{0_R\} \Rightarrow ab \neq 0_R$

Τότε $m = m_1 \cdot m_2$ με $1 < m_1 < m$, $1 < m_2 < m$

Συνεπώς $m \cdot 1_R = 0 \Rightarrow (m_1 \cdot m_2) \cdot 1_R = 0 \Rightarrow$

$(m_1 \cdot 1_R)(m_2 \cdot 1_R) = 0_R$. Αφού $R$ ακέραια περιοχή έχουμε $m_1 \cdot 1_R = 0$ ή $m_2 \cdot 1_R = 0_R$

ΠΕΡΙΠΤΩΣΗ 1) $m_1 \cdot 1_R = 0$. Έστω $a \in R$. Τότε

$$m_1 \cdot a = m_1 \cdot (1_R \cdot a) = \underbrace{1_R \cdot a + 1_R \cdot a + \ldots + 1_R \cdot a}_{m_1 - \text{φορές}} \overset{\text{επιμ.}}{=}$$

$$\underbrace{(1_R + 1_R + \ldots + 1_R)}_{m_1 - \text{φορές}} a = (m_1 \cdot 1_R) \cdot a = 0_R \cdot a = 0_R.$$

Συνεπώς, ο $R$ έχει χαρακτηριστική $\leq m_1$, αντίφαση αφού $m_1 < m$.

ΠΕΡΙΠΤΩΣΗ 2) $m_2 \cdot 1_R = 0$. Με τα ίδια επιχειρήματα έχουμε αντίφαση.

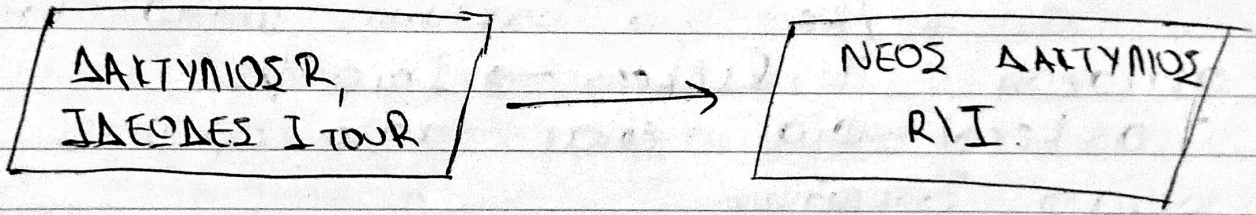
ΠΟΡΙΣΜΑ Αν $R$ σώμα, τότε το $R$ έχει χαρακτηριστική 0. ή $p$ όπου $p$ πρώτος.

ΑΠΟΔΕΙΞΗ Αφού κάθε σώμα είναι ακέραια περιοχή, το αποτέλεσμα έπεται από την προηγούμενη πρόταση.

ΠΡΟΣΟΧΗ Υπάρχουν δακτύλιοι π.χ. ο $\mathbb{Z}_4$ με χαρακτηριστική σύνθετο. Η πρόταση λέει ότι ΔΕΝ υπάρχουν ακέραιες περιοχές με χαρακτηριστική σύνθετο.

## ΔΑΚΤΥΛΙΟΣ ΠΗΛΙΚΟ.

(ΥΠΕΝΘΥΜΙΣΗ: Αν G ομάδα και N κανονική υποομάδα της G τότε ορίσαμε την ομάδα πηλίκο G/N)




ΟΡΙΣΜΟΣ Έστω R δακτύλιος, I ιδεώδες του R. Τότε $(I,+)$ είναι κανονική υποομάδα της αβελιανής ομάδας $(R,+)$ (γιατί κάθε υποομάδα αβελιανής ομάδας είναι κανονική). Άρα ορίζεται η ομάδα πηλίκο $(R/I,+)$. Ορίζω $\cdot : R/I \times R/I \to R/I$

$$(a+I)\cdot(b+I) = (ab)+I$$

ΠΡΟΤΑΣΗ Η πράξη $\cdot$ καλά ορισμένη.

ΑΠΟΔΕΙΞΗ Έστω $a,a',b,b' \in R$ με $a+I=a'+I$ $b+I=b'+I \Rightarrow (a-a') \in I$, $(b-b') \in I$

Έχουμε $ab-a'b' = ab-ab'+ab-a'b' = a(b-b')+(a-a')\cdot b \in I$. [ΙΔΙΑΙ I ιδεώδες]. Άρα $ab+I = a'b'+I$

ΠΡΟΤΑΣΗ $(R/I,+,\cdot)$ ΔΑΚΤΥΛΙΟΣ.

ΑΠΟΔΕΙΞΗ Εύκολη επαλήθευση.

ΠΡΟΣΟΧΗ Αν S δακτύλιος του R ΠΟΥ ΔΕΝ είναι ιδεώδες, τότε το R/S ΔΕΝ είναι δακτύλιος.

ΥΠΕΝΘΥΜΙΣΗ Αν $R_1, R_2$ δακτύλιοι, τότε μια συνάρτηση $\phi: R_1 \to R_2$ λέγεται ομομ. δακτυλίων αν

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

$\phi(ab) = \phi(a)\cdot\phi(b)$ για κάθε $a,b \in R_1$

Τότε θέταμε $\ker\phi = \{a \in R_1 : \phi(a) = 0_{R_2}\}$

ΠΡΟΤΑΣΗ Έστω $R_1, R_2$ δακτύλιοι $\phi: R_1 \to R_2$ ομομ. δακτυλίων. Τότε:

i) $\ker\phi$ ιδεώδες του $R_1$.

ii) $\mathrm{Im}\phi$ υποδακτύλιος του $R_2$.

iii) Έστω $R_1/\ker\phi$ ο δακτύλιος πηλίκο. Τότε η απεικόνιση $T: R_1/\ker\phi \to \mathrm{Im}\phi$ με $T(a+\ker\phi) = \phi(a)$ είναι καλά ορισμένος ισομορφ. δακτυλίων.

ΑΠΟΔΕΙΞΗ i) Από τον ορισμό $(\ker\phi, +)$ υποομάδα του $(R_1, +)$. Έστω $a \in \ker\phi$, $r \in R_1$. Θα δείξουμε $ar \in \ker\phi$ και $ra \in \ker\phi$.

Πράγματι, $\phi(a\cdot r) = \phi(a)\cdot\phi(r) = 0_{R_2}\cdot\phi(r) \overset{\text{ΠΡΟΤ.}}{=\!=} 0_{R_2}$

Ομοίως, $\phi(r\cdot a) = \phi(r)\cdot\phi(a) = \phi(r)\cdot 0_{R_2} \overset{\text{ΠΡΟΤ.}}{=\!=} 0_{R_2}$

ii) Από πρόταση για ομάδες $(\mathrm{Im}\phi, +)$ υποομάδα του $(R_2, +)$. Θα δείξουμε ότι αν $a,b \in \mathrm{Im}\phi$ τότε $ab \in \mathrm{Im}\phi$. Αφού $a \in \mathrm{Im}\phi$ υπάρχει $\tilde{a} \in R_1$ με $a = \phi(\tilde{a})$ ομοίως υπάρχει $\tilde{b} \in R_1$ με $b = \phi(\tilde{b})$

Τότε $ab = \phi(\tilde{a})\cdot\phi(\tilde{b}) = \phi(\tilde{a}\cdot\tilde{b}) \in \mathrm{Im}\phi$. Άρα, $\mathrm{Im}\phi$ υποδ. του $R_2$.

iii) Από πρόταση για ομάδες, T καλά ορισμένος, 1-1, επί και $T(u_1+u_2) = T(u_1) + T(u_2)$ για κάθε $u_1, u_2 \in R_1/\ker\phi$. Μένει να δείξουμε ότι $T(u_1\cdot u_2) = T(u_1)\cdot T(u_2)$

για κάθε $u_1, u_2 \in R_1/\ker\phi$. Πρόχειρα υπάρχουν $a_1, a_2 \in R_1$ με $u_1 = a_1 + \ker\phi$ $u_2 = a_2 + \ker\phi$. Τότε $T(u_1 \cdot u_2) = T((a_1+\ker\phi)\cdot(a_2+\ker\phi)) = T(a_1a_2 + \ker\phi) = \phi(a_1 \cdot a_2) = \phi(a_1)\cdot\phi(a_2) = T(u_1)\cdot T(u_2)$.

ΠΑΡΑΔΕΙΓΜΑ Έστω $n \geq 2$, $R = \mathbb{Z}$ και $I = n\mathbb{Z}$ ιδεώδες του $R$. Περιγράψτε το δακτύλιο πηλίκο $R/I$, δηλ. βρείτε γνωστό δακτύλιο με τον οποίο να είναι ισόμορφο.

ΛΥΣΗ Θα δείξουμε $R/I \cong \mathbb{Z}_n$ ← δακτύλιος ακεραίων modulon.

Έστω $\phi: R/I \to \mathbb{Z}_n$, $\phi(a+I) = [a]_n$

ΙΣΧΥΡΙΣΜΟΣ $\phi$ καλά ορισμένος ισομ. δακτυλίων

ΑΠΟΔΕΙΞΗ Καλά ορισμένος, Έστω $a, a' \in \mathbb{Z}$ με
$a+I = a'+I \Rightarrow a - a' \in I = n\mathbb{Z} \Rightarrow n \mid a-a'$
$\Rightarrow [a]_n = [a']_n$

$\phi((a+I)+(b+I)) = \phi((a+b)+I) = [a+b]_n = [a]_n + [b]_n = \phi(a+I) + \phi(b+I)$

$\phi((a+I)\cdot(b+I)) = \phi(ab+I) = [ab]_n = [a]_n \cdot [b]_n = \phi(a+I)\cdot\phi(b+I)$

$\phi$ ΕΠΙ. Έστω $a \in \mathbb{Z}$. Τότε $[a]_n = \phi(a+I)$. Άρα $\phi$ ΕΠΙ.

$\phi$ 1-1 Έστω $a, a' \in \mathbb{Z}$ με $\phi(a+I) = \phi(a'+I)$
Τότε $[a]_n = [a']_n \Rightarrow [a-a']_n = [0]_n \Rightarrow n \mid a-a'$
$\Rightarrow a - a' \in I \Rightarrow a+I = a'+I$

ΟΡΙΣΜΟΣ Έστω $R$ μεταθετικός δακτύλιος με μονάδα $1_R$ και $I$ ιδεώδες του $R$. Το $I$ λέγεται ΠΡΩΤΟ ιδεώδες του $R$ αν $I \neq R$ και $a \notin I, b \notin I \Rightarrow a \cdot b \notin I$ (δηλ. αν πολλαπλ. δύο στοιχεία που ΔΕΝ είναι στο $I$, τότε και το γινόμενο τους ΔΕΝ είναι στο $I$)

ΠΑΡΑΔΕΙΓΜΑ 1) Είναι το ιδεώδες $I=\mathbb{Z}$ του δακτυλίου $\mathbb{Z}$ πρώτο; ΟΧΙ, διότι απο πρώτα ιδεώδη $I \neq R$.

2) Είναι το ιδεώδες $I=4\mathbb{Z}$ του δακτυλίου $\mathbb{Z}$ πρώτο. ΟΧΙ, διότι $2 \notin I$, $2 \notin I$ αλλά $2 \cdot 2 = 4 \in I$

3) Είναι το ιδεώδες $I=2\mathbb{Z}$ του δακτυλίου $\mathbb{Z}$ πρώτο; ΝΑΙ, διότι α) $1 \in \mathbb{Z} \setminus I$, άρα $I \neq \mathbb{Z}$
β) Έστω $a,b \in \mathbb{Z} \setminus I$. Τότε $a,b$ περιττοί $\Rightarrow$ $a,b$ περιττός $\Rightarrow ab \notin I$.

ΠΡΟΤΑΣΗ \ ΠΑΡΑΔΕΙΓΜΑ Έστω $n \geq 0$ και $I=n\mathbb{Z}$. Τότε το $I$ είναι πρώτο ιδεώδες του $\mathbb{Z}$ αν και μόνο αν $n=0$ ή $n \geq 2$ πρώτος.

ΑΠΟΔΕΙΞΗ Αν $n=0$. Τότε $I=0\mathbb{Z}=\{0\} \neq \mathbb{Z}$ και αν $a \notin I, b \notin I \Rightarrow a \neq 0, b \neq 0 \Rightarrow ab \neq 0$ $\Rightarrow ab \in I$. Άρα $0\mathbb{Z}$ πρώτο ιδεώδες του $\mathbb{Z}$.
Έστω $n \in \mathbb{Z}$ πρώτος. Τότε $I=n\mathbb{Z} \neq \mathbb{Z}$. Έστω $a,b \notin I$ με $ab \in I$. Αφού $ab \in I \Rightarrow n \mid ab \underset{n \text{ πρώτο}}{\Longrightarrow} n \mid a$ ή $n \mid b$
$\Rightarrow a \in I$ ή $b \in I$ αντίφαση.
Άρα $n$ πρώτος $\Rightarrow n\mathbb{Z}$ πρώτο ιδεώδες του $\mathbb{Z}$.
Αν $n=1$, τότε $n\mathbb{Z}=1\mathbb{Z}=\mathbb{Z}$, άρα όχι πρώτο ιδεώδες. Έστω $n \geq 2$ απο $\mathbb{Z}$ σύνθετος. Άρα υπάρχουν $m_1, m_2 \in \mathbb{Z}$ με $1 < m_1 < n$, $1 < m_2 < n$ και $n = m_1 m_2$
Τότε $m_1 \notin n\mathbb{Z}$, $m_2 \notin n\mathbb{Z}$, αλλά $m_1 m_2 = n \in n\mathbb{Z} = I$
Άρα $n\mathbb{Z}$ ΟΧΙ πρώτο ιδεώδες του $\mathbb{Z}$.