23/5/2018

ΔΙΟΡΘΩΣΗ φυλ. 6 ασκ. 6 Έστω R πεπερ. δακτύλιος με μοναδιαίο 1_R και τουλάχιστον δύο στοιχεία.

ΠΡΩΤΑ ΙΔΕΩΔΗ

Υπενθύμιση: Έστω R μεταθ. δακτυλίου $R \neq \{1_R\}$ με μοναδα 1_R και I ιδεώδες του R. Το I λέγεται ΠΡΩΤΟ αν $I \neq R$ και $a,b \notin I \Rightarrow ab \notin I$.

ΠΡΟΤΑΣΗ Έστω $R \neq \{0_R\}$ μεταθ. δακτυλίων με 1_R και I ιδεώδες του R. Τ.Α.Ε.Ι.

i) I πρώτο ιδεώδες

ii) R/I ΑΚΕΡΑΙΑ ΠΕΡΙΟΧΗ

ΑΠΟΔΕΙΞΗ i) $\Rightarrow$ ii) Ισχυρ. 1) Το R/I έχει τουλάχιστον δύο στοιχεία.

Αποδ. Ισχυρ. 1 Αφού I πρώτο $\Rightarrow I \neq R \Rightarrow R/I$ έχει τουλάχιστον δύο στοιχεία γιατί υπάρχει $a \in R/I$ και $a+I \neq 0+I$.

Ισχυρ. 2) Έστω $u_1, u_2 \in R/I$ μη μηδενικά. Τότε $u_1 \cdot u_2 \neq 0$ στο R/I

ΑΠΟΔΕΙΞΗ Υπάρχουν $a_1, a_2 \in R$ με $u_1 = a_1 + I$ και $u_2 = a_2 + I$. Αφού $u_1 \neq 0$ στο R/I έχουμε $a_1 \notin I$. Ομοίως $a_2 \notin I$. Άρα αφού I πρώτο $a_1 \cdot a_2 \notin I$. Συνεπώς, $a_1a_2 + I$ μη μηδενικό στο R/I. Αλλά $u_1 u_2 = (a_1+I)(a_2+I) = a_1a_2 + I$. Άρα u_1u_2 μη μηδενικό στο R/I. Συνεπώς, R/I ακερ. περιοχή γιατί είναι μεταθ. δακτύλιος. (αφού ο R είναι μεταθετικός) με ουδέτερο ως προς τον πολλαπλασιασμό το $1_R + I$.

ii) $\Rightarrow$ i) Υποθέτουμε R/I Ακερ. Περιοχή. Θ.δ.ο. I πρώτο ιδεώδες του R.

Ισχυρ. 1) $I \neq R$.

Απόδειξη Αν $I = R \Rightarrow R/I$ έχει μόνο ένα στοιχείο, αντίφαση γιατί εξ ορισμού μια ακέραια περιοχή έχει τουλάχιστον δύο στοιχεία.

Ισχυρισμός 2) Αν $a,b \in R$ με $a \notin I$ και $b \notin I$ τότε $ab \notin I$

Απόδειξη Έστω $ab \in I$. Τότε $a \notin I \Rightarrow a+I$ μη μηδ. στο R/I
$b \notin I \Rightarrow b+I$ " " " "

Αφού $ab \in I \Rightarrow ab+I = 0+I$.
Άρα $a+I \neq 0+I$ $b+I \neq 0+I$ αλλά
$(a+I)(b+I) = 0+I$. Αντίφαση, αφού R/I Ακέραια περιοχή

ΟΡΙΣΜΟΣ Έστω R μεταθ. δακτύλιος με μονάδα 1_R και I ιδεώδες του R. Το I λέγεται ΜΕΓΙΣΤΟΤΙΚΟ (maximal) αν $I \neq R$ και ΔΕΝ υπάρχει ιδεώδες J του R με $I \subsetneq J \subsetneq R$.

(Με άλλα λόγια, πρέπει $I \neq R$ και το μόνο ιδεώδες του R που περιέχει γνήσια το I να είναι ο R)

ΠΑΡΑΔΕΙΓΜΑ 1) Είναι το ιδεώδες $I = 4\mathbb{Z}$ του δακτυλίου $\mathbb{Z}$ μεγιστοτικό; ΟΧΙ, διότι για $J = 2\mathbb{Z}$ έχουμε J ιδεώδες του $\mathbb{Z}$ με $I \subsetneq J \subsetneq \mathbb{Z}$

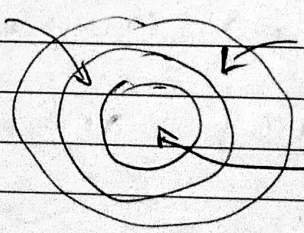
ΔΗΛ. I υποσύνολο του J και $I \neq J$

ΙΣΧΥΕΙ διότι κάθε πολλαπλάσιο του 4 είναι πολλ. και του 2 ∈ J και $2 \notin I$

ΠΡΟΤΑΣΗ Έστω R μεταθετικός δακτύλιος με μονάδα 1_R και I ιδεώδες του R. Τ.Α.Ε.Ι
i) I μεγιστοτικό ιδεώδες του R
ii) Ο δακτύλιος πηλίκο R/I είναι σώμα.
(ΧΩΡΙΣ ΑΠΟΔΕΙΞΗ)

ΠΟΡΙΣΜΑ Έστω R μεταθ. δακτύλιος με μονάδα 1_R. Κάθε μεγιστοτικό ιδεώδες του R είναι πρώτο.

ΑΠΟΔΕΙΞΗ Έστω I μεγιστοτικό ιδεώδες του $R \Rightarrow$
ΠΡΟΤΑΣΗ
$\Longrightarrow$ R/I ΣΩΜΑ $\Longrightarrow$ R/I ΑΚΕΡΑΙΑ ΠΕΡΙΟΧΗ.
ΠΡΟΤ.
$\Longrightarrow$ I ΠΡΩΤΟ ΙΔΕΩΔΕΣ.



ΠΡΟΣΟΧΗ Το ιδεώδες $I=0\mathbb{Z}=\{0\}$ του δακτυλίου $\mathbb{Z}$ είναι πρώτο (το έχουμε δει) αλλά δεν είναι μεγιστικό διότι για $J=2\mathbb{Z}$ έχουμε $I \subsetneq J \subsetneq \mathbb{Z}$.

ΠΡΟΤΑΣΗ Ένα ιδεώδες I του $\mathbb{Z}$ είναι μεγιστικό αν και μόνο αν υπάρχει πρώτος p με $I=p\mathbb{Z}$

ΑΠΟΔΕΙΞΗ ΙΣΧΥΡ. 1) Έστω p πρώτος. Τότε το $I=p\mathbb{Z}$ είναι μεγιστικό ιδεώδες του $\mathbb{Z}$.
ΑΠΟΔΕΙΞΗ Έστω ότι δεν ισχύει. Υπάρχει ιδεώδες J του $\mathbb{Z}$ με $I \subsetneq J \subsetneq \mathbb{Z}$ θα βρούμε αντίφαση.
Αφού $p \in I$ και $I \subseteq J \Rightarrow p \in J$.
Αφού $I \subsetneq J$ υπάρχει $a \in J$ ώστε $p \nmid a$. Άρα ΜΚΔ$(a,p)=$
Άρα από θ. Αριθμών υπάρχουν $x_1, x_2 \in \mathbb{Z}$ με $1 = x_1 a + x_2 p$.
Αφού J ιδεώδες και $p, a \in J \Rightarrow 1 \in J$
Έστω $c \in \mathbb{Z}$. Τότε $c = c1 \in J$. Άρα $J=\mathbb{Z}$ αντίφαση
ΙΣΧΥΡ. 2) Αν I μεγιστικό ιδεώδες του $\mathbb{Z}$, τότε υπάρχει πρώτος p με $I=p\mathbb{Z}$.
ΑΠΟΔΕΙΞΗ Έστω ότι δεν υπάρχει τέτοιος πρώτος. Αφού I μεγιστικό, από πρόταση I πρώτο ιδεώδες του $\mathbb{Z}$. Αλλά έχουμε υπολογίσει όλα τα πρώτα ιδεώδη του $\mathbb{Z}$ είναι το $0\mathbb{Z}=\{0\}$ ή $I=p\mathbb{Z}$ για κάποιο πρώτο p. Αντίφαση, διότι το το $\{0\}$ είδαμε δεν είναι μεγιστικό ιδεώδες του $\mathbb{Z}$.

ΣΥΜΠΕΡΑΣΜΑ 1. Αν I ιδεώδες του $\mathbb{Z}$ υπάρχει μοναδικός ακέραιος $m \geq 0$ ώστε $I=m\mathbb{Z}$
2. I πρώτο $\Leftrightarrow$ $m=0$ ή $m \geq 2$ πρώτος
3. I μεγιστικό $\Leftrightarrow$ $m \geq 2$ πρώτος

Συνεπώς το μόνο ιδεώδες I του $\mathbb{Z}$ που είναι πρώτο αλλά ΟΧΙ ΜΕΓΙΣΤΟΤΙΚΟ είναι το $\{0\}=0\mathbb{Z}$
ΠΟΡΙΣΜΑ Έστω $n \geq 2$. Τότε Τ.Α.Ε.Ι.
i) $\mathbb{Z}_n$ ακέραια περιοχή
ii) $\mathbb{Z}_n$ σώμα
iii) n πρώτος.

ΑΠΟΔΕΙΞΗ Αφού $\mathbb{Z}_n$ είναι ισόμορφος με το δακτύλιο πηλίκο $\mathbb{Z}/n\mathbb{Z}$ το αποτέλεσμα έπεται.

ΠΡΟΣΟΧΗ Το $\mathbb{Z}$ ακέραια περιοχή που δεν είναι σώμα.

ΠΟΛΥΩΝΥΜΑ Έστω R μεταθ. δακτύλιος με μονάδα θα ορίσουμε έναν νέο δακτύλιο $R[X]$ που το λέμε δακτύλιο πολυωνύμων του R σε "μία μεταβλητή" X.

ΑΝΕΠΙΣΗΜΑ $R[X] = \{a_0 + a_1X + \dots + a_sX^s : s \geq 0, a_i \in R\}$ με πράξεις $+, \cdot$ που όλοι γνωρίζουμε.

ΕΠΙΣΗΜΟΣ ΟΡΙΣΜΟΣ του $R[X]$

$R[X] = \{$ σύνολο ακολουθιών $(a_n)_{n\geq 0}$ με $a_n \in R$ για κάθε n και υπάρχει N_0 ώστε $a_m = 0$ για κάθε $m \geq N_0 + 1\}$

Ορίζουμε δύο πράξεις $+$ και $\cdot$ στο $R[X]$

$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (c_n)_{n\geq 0}$ με $c_i = a_i + b_i$ για κάθε i.

Πολλαπλασιασμός $(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (d_n)_{n\geq 0}$

όπου για $r \geq 0$ $d_r = \sum_{i=0}^{r} a_i \cdot b_{r-i}$

Παράδειγμα $d_0 = a_0 \cdot b_0$, $d_1 = a_0b_1 + a_1b_0$

$d_2 = a_0b_2 + a_1b_1 + a_2b_0$ κλπ.

Πρόταση i) $R[X]$ μεταθετικός δακτύλιος με μονάδα το $(1, 0, 0, 0, 0, \dots)$

ii) Θέτουμε $x = (0, 1, 0, 0, 0, \dots)$

Τότε $x^2 = (0, 0, 1, 0, 0 \dots)$

$x^3 = (0, 0, 0, 1, 0, \dots)$

ΟΡΙΣΜΟΣ Έστω $(a_n)_{n\geq 0} \in R[X]$ μη μηδενικό. Τότε υπάρχει μοναδικό r ώστε $a_r \neq 0$ και $a_i = 0$ για $i \geq r+1$. Λέμε το r βαθμό του $(a_n)_{n\geq 0}$ π.χ. Αν $R = \mathbb{Z}$ και $(a_n)_{n\geq 0}$. Τότε το $(a_n)_{n\geq 0}$ έχει βαθμό 4.

Παρατηρούμε επίσης ότι $(2, 3, 5, 7, 9, 0, 0, 0, \dots) = 2 + 3x + 5x^2 + 7x^3 + 9x^4$.

όπου $x=(0,1,0,0,0,\dots)$ όπως προηγουμένως.
Εύκολα βλέπουμε. Έστω $(a_n)_{n\geq 0}$ μη μηδενικού βαθμού $r\geq 0$. Τότε $(a_n)_{n\geq 0} = a_0+a_1x+\dots+a_rx^r$
Ο ορισμός είναι διαδεδομένος και πολύ χρήσιμος.

ΠΡΟΤΑΣΗ Έστω R ακέραια περιοχή και $p_1(x), p_2(x)\in R[x]$ δύο μη μηδενικά πολυώνυμα. Τότε το πολυώνυμο $p_1(x)\cdot p_2(x)$ είναι μη μηδενικό και ισχύει $\deg(p_1(x)\cdot p_2(x)) = \deg p_1(x) + \deg p_2(x)$

ΑΠΟΔΕΙΞΗ Έστω $d_1=\deg p_1(x)$, $d_2=\deg p_2(x)$
Τότε $p_1(x)=a_0+a_1x+\dots+a_{d_1}x^{d_1}$ με $a_i\in R$ και $a_{d_1}\neq 0$
και $p_2(x)=b_0+b_1x+\dots+b_{d_2}\cdot x^{d_2}$ με $b_j\in R$ και $b_{d_2}\neq 0$
Τότε από τον ορισμό του πολλαπλασιασμού πολυωνύμων $p_1(x)\cdot p_2(x) = a_0b_0+(a_0b_1+a_1b_0)x^2+\dots+a_{d_1}b_{d_2}x^{d_1+d_2}$
Αφού R ακέραια περιοχή και $a_{d_1}\neq 0$, $b_{d_2}\neq 0 \Rightarrow$ $a_{d_1}b_{d_2}\neq 0$. Επομένως, το $p_1(x)p_2(x)$ είναι μη μηδενικού βαθμού d_1+d_2.

ΠΡΟΣΟΧΗ Αν R όχι ακέραια περιοχή πιθανά πράγματα μπορούν να συμβούν.

ΠΑΡΑΔΕΙΓΜΑ $R=\mathbb{Z}_4$. Τότε αν $p_1(x)=[1]_4+[2]_4x^2$ και $p_2(x)=[2]_4\cdot x^3$. Έχουμε $\deg p_1(x)=2$, $\deg p_2(x)=3$
$p_1(x)\cdot p_2(x) = ([1]_4+[2]_4x^2)\cdot([2]_4\cdot x^3) =$
$[1]_4\cdot[2]_4x^3+[2]_4\cdot[2]_4\cdot x^5 = [2]_4\cdot x^3$
Άρα, $\deg(p_1(x)\cdot p_2(x)) = 3 \neq 5 = \deg p_1(x)+\deg p_2(x)$.