Μάθημα 20ο 13/05/16

R δακτύλιος (ring)

$\mathbb{Z}, \mathbb{Z}_6, \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$M(n\times n, \mathbb{R}), M(n\times n, \mathbb{Z}_6)$

$\varphi: \mathbb{Z} \to \mathbb{Z}$

$1 \mapsto a \qquad \varphi(1)=a$

$1\cdot 1 \mapsto a\cdot a \qquad \varphi(1\cdot 1)=\varphi(1)\varphi(1) = a\cdot a$

$\overset{\shortparallel}{\varphi(1)} = a$

$a^2 = a \Leftrightarrow a(a-1)=0 \Leftrightarrow a=0$ ή $a=1$

$\varphi(1)=0$ τετριμ.

$\varphi(1)=1$ ταυτοτικός

$\varphi: \mathbb{Z}_p \to \mathbb{Z}_p$

$1 \mapsto a$

$1\cdot 1 \mapsto a\cdot a \qquad \varphi(1\cdot 1)=\varphi(1)\cdot\varphi(1)=a\cdot a$

$\overset{\shortparallel}{\varphi(1)} = a$

$a(a-1) \equiv 0 \bmod p \Leftrightarrow a(a-1) = \kappa p$

$p \mid a$ ή $a-1$ και p πρώτος

$a<p$.

Άρα, $a=0$ ή $a=1$

$\varphi: \mathbb{Z}_p \to \mathbb{Z}_p$

$1 \mapsto 0$ τετριμμ.

$1 \mapsto 1$ ταυτοτικός

$\Phi: \mathbb{Z}_6 \to \mathbb{Z}_6$

$1 \mapsto a$

$a(a-1) \equiv 0 \bmod 6$

$a(a-1) \equiv \kappa 6$

$a=3 \quad a-1=2$

$a=4 \quad a-1=3$

$\Phi: \mathbb{Z}_6 \to \mathbb{Z}_6$

$1 \mapsto 0$

$1 \mapsto 1$

$1 \mapsto 3$

$1 \mapsto 4$.

$\mathbb{Q} = \{ \frac{a}{r} \mid a, r \in \mathbb{Z},\ r \neq 0 \}$

$\mathbb{N} \xrightarrow[\text{επι}]{1-1} \mathbb{Z} \xrightarrow[\text{επι}]{1-1} \mathbb{Q} \xrightarrow[\text{επι}]{\cancel{1-1}} \mathbb{R}$

ΕΡΩΤΗΜΑ:

$\mathbb{Q} \cong \mathbb{R}$ σαν δακτύλιοι; <u>ΟΧΙ</u>.

$\exists \Phi: \mathbb{Q} \cong \mathbb{R}$

$1 \mapsto 1$

$a \mapsto \sqrt{2} = \Phi(a)$

$a^2 \mapsto (\sqrt{2})^2 = 2$

$2 \mapsto 2$

$a \in \mathbb{Q}$ και $a^2 = 2$ στο $\mathbb{Q}$ αδύνατο.

<u>ΠΟΛΥΩΝΥΜΙΚΟΙ ΔΑΚΤΥΛΙΟΙ</u>

R τυχαίος δακτύλιος (εκτός αν τον ορίσουμε)

$f: \mathbb{R} \to \mathbb{R}$

$x \mapsto ax^2 + \beta x + \gamma$

πολυωνυμική συνάρτηση

<u>ΟΡΙΣΜΟΣ</u>: Έστω R δακτύλιος. Ένα πολυώνυμο ως προς X με συντελεστές στον R είναι μια παράσταση μορφής : $a_0 + a_1X + a_2X^2 + \dots + a_nX^n + 0X^{n+1} + \dots$ ώστε $a_i \in R$ και $\exists n \in \mathbb{N}$ με $a_\kappa = 0_R$ για $\kappa > n$.

<u>ΠΑΡΑΤΗΡΗΣΗ</u>: Αν $a_n \neq 0$ και $a_\kappa = 0$ για $\kappa > n$ συνήθως γράφουμε μέχρι το a_nX^n δηλ $a_0 + a_1X + \dots + a_nX^n$.

Θα λέμε ότι δύο πολυώνυμα $a_0 + a_1X + \dots$, $b_0 + b_1X + \dots$ είναι **ίσα** <u>ανν</u> $a_i = b_i$, $\forall i$

Συμβολίζουμε $f(x) = a_0 + a_1X + \dots$

Με τη βοήθεια ενός πολυωνύμου, ορίζεται πολυωνυμική συνάρτηση

$f: R \to R$ με τύπο $f(a) = a_0 + a_1a + a_2a^2 + \dots$

ΠΑΡΑΔΕΙΓΜΑ: $R=\mathbb{Z}_2$, $f(x)=0+0\cdot x+0\cdot x^2+\cdots$

$g(x)=0+1\cdot x+1\cdot x^2+0\cdot x^3+\cdots$

$f(0)=0=f(1)$

$g(0)=0=g(1)$

Αλλά $g(x)\neq f(x)$.

ΠΡΟΣΟΧΗ: Αν ο R είναι μοναδιαίος αντί για $1_R\cdot x^k$ γράφουμε μόνο x^k επίσης $0_R\cdot x^k=0_R$

ΟΡΙΣΜΟΣ: Το σύνολο όλων των πολυωνύμων με συντελεστές από το δακτύλιο R και μεταβλητή x καλείται **πολυωνυμικός δακτύλιος** και συμβολίζεται $R[x]$.

ΠΡΟΤΑΣΗ: Στο $R[x]$ ορίζουμε δύο πράξεις: $(a_0+a_1x+\cdots)+(b_0+b_1x+\cdots)=c_0+c_1x+\cdots$

με $c_i=a_i+b_i$, $i\in\mathbb{N}$

$(a_0+a_1x+\cdots)\cdot(b_0+b_1x+\cdots)=c_0+c_1x+\cdots$ με $c_i=\sum_{k=0}^{i}a_k b_{i-k}$, $i\in\mathbb{N}$ ⊕

Με αυτές τις πράξεις και αυτές που κληρονομεί από τον R, το σύνολο $R[x]$ αποτελεί δακτύλιο.

Προσοχή στο γινόμενο $c_0=a_0b_0$, $c_1=a_0b_1+a_1b_0$, $c_2=a_0b_2+a_1b_1+a_2b_0+\cdots$

Το μηδενικό στοιχείο στον $R[x]$: $0_{R[x]}=0_R+0_Rx+0_Rx^2+\cdots$

Τα πολυώνυμα μορφής a_ix^i καλούνται μονώνυμα. Άρα, ένα πολυώνυμο είναι άθροισμα μονωνύμων.

Αν ο R είναι μοναδιαίος, τότε $1_R\cdot x^k=x^k$.

ΙΔΙΟΤΗΤΕΣ:

1) Αν ο R είναι μοναδιαίος και ο $R[x]$ είναι μοναδιαίος.
2) Αν είναι αντιμεταθετικός, και ο $R[x]$ είναι αντιμεταθετικός
3) Αν ο R είναι ακέραια περιοχή και ο $R[x]$ είναι ακέραια περιοχή

ΑΠΟΔΕΙΞΗ:

3) Έστω $f(x), g(x) \in R[x]$ με $f(x), g(x) \neq 0$ και $f(x) \cdot g(x) = 0$

$f(x) \neq 0 \Rightarrow \exists a_n \neq 0$ και $a_k = 0$, $k > n$

$g(x) \neq 0 \Rightarrow \exists b_l \neq 0$ και $b_k = 0$, $k > l$.

$f(x) \cdot g(x) = c(x)$

$c(x) = c_0 + c_1 \cdot x + \dots$

$$c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

$$c_{n+l} = \sum^{n+l} a_k b_{n+l-k}$$

$n=2$, $l=3$ $\qquad$ $a_2, b_3 \neq 0$ και R ακέραια περιοχή

$n+l=5$ $\qquad$ $\neq 0$

$$c_5 = \underset{0}{a_0 b_5} + \underset{0}{a_1 b_4} + \boxed{a_2 b_3} + \underset{0}{a_3 b_2} + \underset{0}{a_4 b_1} + \underset{0}{a_5 b_0}.$$

Αφού $c_5 = a_2 b_3 \neq 0 \Rightarrow c_0 + c_1 x + \dots \neq 0$ και έχουμε υποθέσει ότι είναι μηδέν

Άρα, ή το $f(x)$ ή $g(x)$ είναι μηδέν.

ΟΡΙΣΜΟΣ: Ο βαθμός του μηδενικού πολυωνύμου δεν ορίζεται. Συμβολισμός $\deg(f) = n$.

Ο βαθμός του $a_0 + a_1 x + \dots \neq 0$ είναι το n, όταν $a_n \neq 0$ και $a_i = 0$ για $i > n$

ΠΡΟΤΑΣΗ: Αν $f(x), g(x) \in R[x]$ τότε:

1) $\deg(f(x) \cdot g(x)) = \deg(f) + \deg(g)$, όταν $f(x), g(x) \neq 0$ και R ακέραια περιοχή.

2) $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$ και $f(x) + g(x) \neq 0$.

ΠΑΡΑΔΕΙΓΜΑ: $R = \mathbb{Z}_6$.

$2x^2 = f(x)$, $3x^5 = g(x)$ $\qquad$ $2x^2 \cdot 3x^5 = 6x^7 \equiv 0 \mod 6$.

ΘΕΩΡΗΜΑ (Αλγόριθμος της διαίρεσης): Έστω $\mathbb{F}$ σώμα και $f(x), g(x) \in \mathbb{F}[x]$. Αν $g(x) \neq 0$, τότε υπάρχουν μοναδικά $\pi(x), u(x) \in \mathbb{F}[x]$ ώστε $f(x) = \pi(x) \cdot g(x) + u(x)$ και $u(x) = 0$ ή $\deg u(x) < \deg(g(x))$.

ΑΠΟΔΕΙΞΗ: Με επαγωγή στο βαθμό του $f(x)$.

Αν $f(x)=0$ ή $\deg f(x)<\deg(g(x))$ τότε $\Pi(x)=0$ και $f(x)=U(x)$.

Αν $\deg f(x)=\deg g(x)$

$f(x)=a_0+a_1x+\cdots+a_nx^n$

$g(x)=b_0+b_1x+\cdots+b_kx^k$

$$f(x)=a_nb_n^{-1}g(x)+\underbrace{(f(x)-a_nb_n^{-1}g(x))}_{=U(x)}$$

$\deg(f(x)-a_nb_n^{-1}g(x))<n$

Υποθέτουμε ότι η πρόταση ισχύει για βαθμούς $\leq n$.

Έχουμε $n>k$

$\deg(a_nb_k^{-1}x^{n-k}g(x))=\deg f(x)$ και έχουν τον ίδιο συντελεστή

$f(x)=a_nb_k^{-1}x^{n-k}g(x)+(f(x)-a_nb_k^{-1}x^{n-k}g(x))$

Έστω $h(x)=a_nb_k^{-1}x^{n-k}g(x)$, $\deg h(x)<n$ εφαρμόζεται η επαγωγή:

$h(x)=\Pi'(x)\cdot g(x)+U'(x)$ με $U'(x)=0$ ή $\deg U'(x)<\deg g(x)$

$$f(x)=a_nb_k^{-1}x^{n-k}g(x)+h(x)=a_nb_k^{-1}x^{n-k}g(x)+\Pi'(x)\cdot g(x)+U'(x)=$$
$$=\underbrace{(a_nb_k^{-1}x^{n-k}+\Pi'(x))}_{\Pi(x)}g(x)+U'(x)=\Pi(x)\cdot g(x)+U'(x)$$

Μοναδικότητα:

$f(x)=\Pi_1(x)\cdot g(x)+U_1(x)=\Pi_2(x)g(x)+U_2(x)$

$U_2(x)=0$ ή $\deg(U_1(x))<k$

$U_2(x)=0$ ή $\deg(U_2(x))<k$

$(\Pi_1(x)-\Pi_2(x))g(x)=U_2(x)-U_1(x)$

Γσώμα $\Rightarrow$ Α.Π. $\Rightarrow$ $F[x]$ Α.Π.

Αν $\pi_1(x) \neq \pi_2(x)$ και $v_2(x) \neq v_1(x)$.
Αλλά έχουν διαφορετικούς βαθμούς. Αδύνατο

Αν $v_1(x) = v_2(x) \overset{\oplus}{\Rightarrow} \pi_1(x) = \pi_2(x)$

ΘΕΩΡΗΜΑ: Εστω $\mathbb{F}$ σώμα και $f(x) \in \mathbb{F}[x]$. Αν θεωρήσουμε την πολυωνυμική συνάρτηση $f: \mathbb{F} \to \mathbb{F}$ και $f(a) = 0$, αvv το $(x-a)$ διαιρεί ακριβώς το $f(x)$

ΑΠΟΔΕΙΞΗ:
"$\Leftarrow$": $f(x) = (x-a)\pi(x) \Rightarrow f(a) = (a-a)\pi(a) = 0$
"$\Rightarrow$": Διαιρούμε το $f(x)$ με το $x-a$
$f(x) = (x-a)\pi(x) + v(x)$
$v(x) = 0$ ή $\deg(v(x)) < 1 \Rightarrow v(x) = \beta$
$0 = f(a) = (a-a)\pi(a) + \beta \Rightarrow \beta = 0$.

ΘΕΩΡΗΜΑ: Εστω $\mathbb{F}$ σώμα και $f(x) \in \mathbb{F}[x]$ βαθμού n, τότε το $f(x)$ θα έχει το πολ[illegible] n ρίζες διακεκριμμένες.

ΑΠΟΔΕΙΞΗ: Εστω ότι έχει περισσότερες. Με επαγωγή στο βαθμό:
$\deg f(x) = 0 \Rightarrow f(x) = \beta$, άρα έχει καμία ρίζα.
$\deg f(x) = 1 \Rightarrow f(x) = ax + \beta$ έχει μια ρίζα

Υποθέτουμε ότι η πρόταση ισχύει για βαθμό $<n$.
Εστω ότι το $f(x)$ έχει $\{a_1, a_2, \dots, a_n, a_{n+1}\}$ διακεκριμμένες ρίζες.
Άρα, $f(a_i) = 0$, $i = 1, \dots, n+1$.
$f(x) = (x-a_i)\pi(x) + v(x)$
$v(x) = 0$ και $\deg \pi(x) < n$.
Επίσης, $\pi(a_i) = 0$, $i = 2, \dots, n+1$.
Άρα το $\pi(x)$ έχει περισσότερες διακεκριμμένες ρίζες από το βαθμό του.
Άτοπο από επαγωγή

ΠΟΡΙΣΜΑ: Έστω $\mathbb{F}$ σώμα και το $\mathbb{F}$ έχει άπειρα στοιχεία. Αν $f(x) \in \mathbb{F}[x]$ και μηδενίζεται για άπειρες τιμές από το $\mathbb{F}$, τότε $f(x) = 0$.

ΑΠΟΔΕΙΞΗ: Αν $f(x) \neq 0$ τότε θα έχει το πολύ n διακεκριμμένες ρίζες. Αλλά αυτό δεν ισχύει από την υπόθεση. Άρα, $f(x) = 0$.