Μαθημα 22º 30/5/2017

Δομες

R αντιμ. μοναδ. και $I \triangleleft R$

I μεγιστο $\Leftrightarrow R/I$ σωμα

$R = \mathbb{F}[x]$ πολυωνυμικος δακτυλιος, $\mathbb{F}$ σωμα

$\mathbb{F}[x]$ αντιμετ. μοναδ.

$I \triangleleft \mathbb{F}[x]$ τυχαιο

↓

τα στοιχεια του πολλαπλασια ενος πολυωνυμου

$\mathbb{F} = \mathbb{Q}$ $\mathbb{Q}[x]$, $5 \in I \triangleleft \mathbb{Q}[x] \Rightarrow$ τοτε και ολα τα πολλαπλασια ανηκουν

$\frac{1}{5} \cdot 5 \in I \Rightarrow 1 \in I \Rightarrow f(x) \cdot 1 \in I \quad \forall f(x)$

Προταση

Αν $I \triangleleft \mathbb{F}[x]$, τοτε $\exists f(x) \in I$ ωστε $I = \langle f(x) \rangle$

Αποδειξη

$I = \langle f(x) \rangle = \{ f(x) g(x) \mid g(x) \text{ τυχαιο} \}$

$I \subseteq \mathbb{F}[x]$. Ονομαζουμε $S = \{ n \mid n \in \mathbb{N} \text{ και } n = \deg g(x),\ g(x) \in I \}$

$S \subseteq \mathbb{N} \Rightarrow$ Υπαρχει ελαχιστο στοιχειο $\in S \Leftrightarrow \exists f(x) \in I$ με

$\deg(f(x)) = k \leq \deg(h(x)) \quad \forall h(x) \in I$

Εμεις θδο $I = \langle f(x) \rangle$

Προφανως ισχυει οτι $I \supseteq \langle f(x) \rangle$. Υποθετουμε λοιπον οτι υπαρχει αλλο ενα στοιχειο που δεν ανηκει εκει μεσα. Εστω $g(x) \in I - \langle f(x) \rangle$

$\Rightarrow g(x) = \pi(x) f(x) + \upsilon(x)$ με $\upsilon(x) \neq 0$ και $\deg(\upsilon(x)) < k$

$\underbrace{g(x)}_{\in I} - \underbrace{\pi(x) f(x)}_{\in I} \in I \Rightarrow \upsilon(x) \in I$ ομως $\deg(\upsilon(x)) < k = \min S$ Αδυνατο!

Αρα το $I = \langle f(x) \rangle$ δηλ. γενναται απο ενα πολυωνυμο δεν σπάει σε πολυώνυμα μικρού βαθμού

Θεώρημα

Έστω $I \triangleleft \mathbb{F}[x]$, I μέγιστο αν.ν $I = \langle f(x) \rangle$ με $f(x)$ ανάγωγο

Απόδειξη

$I \triangleleft \mathbb{F}[x] \Rightarrow I = \langle f(x) \rangle$ για κάποιο $f(x) \in \mathbb{F}[x]$

Υποθέτουμε όχι I μέγιστο και $f(x) = g(x)h(x)$ όχι ανάγωγο

Εφόσον όχι ανάγωγο τότε $g(x) \neq$ σταθερό θα έχω τότε $f(x) \in \langle g(x) \rangle$

$\Rightarrow I \subsetneq \langle g(x) \rangle \subsetneq \mathbb{F}[x]$

Αδύνατο αφού το I μέγιστο

Υποθέτουμε ότι $f(x)$ ανάγωγο. Να δείξουμε ότι $I = \langle f(x) \rangle$ μέγιστο

Έστω I όχι μέγιστο τότε $I \subsetneq J \subsetneq \mathbb{R}[x]$

όμως $J \triangleleft \mathbb{R}[x] \Rightarrow J = \langle h(x) \rangle$

Τότε $f(x) \in I \subset \langle h(x) \rangle = J \Rightarrow f(x) = h(x)g(x)$ για κάποιο μη σταθερό $g(x)$

Άρα $f(x)$ ανάγωγο, αδύνατο αφού $f(x) = h(x)g(x)$ για μη σταθερό $g(x)$

Πόρισμα

Αν $f(x) \in \mathbb{F}[x]$ είναι ανάγωγο τότε $\mathbb{F}[x] / \langle f(x) \rangle$ είναι σώμα

Ερώτημα

Με τι μοιάζουν αυτά τα σώματα;

Παρατήρηση $\mathbb{F}$ "$\subseteq$" $\mathbb{F}[x] / \langle f(x) \rangle$ σώμα; → έχει σύμπλοκα

(?) → έχει πολυώνυμα

$\forall a \in \mathbb{F}$ "$\subseteq$" $\mathbb{F}[x]$

$a + I \in \mathbb{F}[x] / I$

⊛ $\bar{a} = a + I$ ορίζεται μονομορφισμός δακτυλίων $\phi : \mathbb{F} \rightarrowtail \mathbb{F}[x]/I$
με τύπο $\phi(a) = \bar{a} = a + I$, μέσω της εμβάπτισης ϕ μπορούμε να θεωρήσουμε ότι $\mathbb{F}$ ζει μέσα στο $\mathbb{F}[x]/I$

πχ. στο πιο απλο σωμα απειρο (τα αλλα $<\infty$)

$\mathbb{F} = \mathbb{Q} \to \mathbb{Q}[x]$ δακτυλιος οχι σωμα

$f(x) = x^2 - 2$ αναγωγο στον $\mathbb{Q}[x]$ βαθμου 2 (το πιο απλο πολυωνυμο)

$A = \mathbb{Q}[x] / \langle x^2 - 2 \rangle = I$ σωμα, $\mathbb{Q}$ "$\subseteq$" A

$A = \{ h(x) + I \mid h(x) \in \mathbb{Q}[x] \}$ (μου φαινεται μεγαλο, θελω ολα τα πολυων;)

Αν εχουμε αλλο ενα $h'(x)$ με $h'(x) - h(x) \in I$ θα $\in I$ οταν θα ειναι πολλαπλασια του $\langle x^2 - 2 \rangle$

$h(x)$ μακρυα απο το I

Αν $\deg h(x) \geq 2 \Rightarrow h(x) = f(x)\pi(x) + u(x)$ $\quad f(x) = x^2 - 2$

$h(x) - f(x)\pi(x) = u(x) \Rightarrow \deg(u(x)) = 0$ ή 1 ή $u(x) = 0$

$h(x) + I = f(x)\pi(x) + u(x) + I = u(x) + I$ το "καπελο" σημαινει $+I$

$A = \{ u(x) + I \mid \deg u(x) \leq 1$ ή $u(x) = 0 \}$

$u(x) = a + bx$ (θα εχει αυτη τη μορφη)

$A = \{ a + bx + I \mid a, b \in \mathbb{Q} \} = \{ \bar{a} + \bar{b}\bar{x} \mid a, b \in \mathbb{Q} \}$

$$\left.\begin{array}{l} \bar{a} = a + I \\ \bar{b} = b + I \\ \bar{x} = x + I \end{array}\right\} \Rightarrow \begin{array}{l} \bar{a} + \bar{b}\bar{x} = a + I + (b + I)(x + I) = a + I + bx + bI + Ix + I^2 = \\ = a + bx + I \end{array}$$

A: Διαν. χωρος διαστασης 2 πανω απο το $\mathbb{Q}$ με στοιχεια I και x

η διασταση εξαρταται απο τη δυναμη του x στην $f(x)$

$\bar{x} \cdot \bar{x} = \overline{x^2} = x^2 + I = x^2 - 2 + 2 + I = \underbrace{(x^2 - 2)}_{\text{βρισκεται μεσα στο } I} + 2 + I = 2 + I = \bar{2}$

Το $\bar{x}$ στο συγκεκριμενο A θα το συμβολιζω με το "συμβολο"

$\sqrt{2} = \bar{x} \to A = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$

Εφτιαξα τη $\sqrt{2}$ τεχνητα μεσα στο $\mathbb{Q}$ (απο ιδεωδη, μεγιστα κτλ)

Κατασκευασα εναν δ.χ με ολους τους δυνατους γραμμικους συνδυασμους

με το 1 και $\sqrt{2}$ εχοντας μικρη επεκταση με το βαθμο 2

ξεκινωντας απο ενα αναγωγο πολυωνυμο

$\mathbb{R}[x]$ $x^2+1=f(x) \in \mathbb{R}[x]$ αναγωγο

$I=\langle f(x)\rangle$ μεγιστο

$\mathbb{R}[x]/I$ σωμα. Ποιο ειναι το σωμα;

$C=\mathbb{R}[x]/I$ $\mathbb{R} \rightarrowtail C$

$C=\{g(x)+I \mid g(x)\in \mathbb{R}[x]\} \to f(x)=x^2+1$

Αν $\deg g(x) \geq 2 \Rightarrow g(x)=f(x)\pi(x)+\upsilon(x)$ $\upsilon(x)=0$ ή $\deg \upsilon(x)=0$ ή $1 \Rightarrow$

$\upsilon(x)=\alpha x \beta x$ με $a^2+\beta^2\neq 0$

$g(x)+I=f(x)\pi(x)+\upsilon(x)+I=\upsilon(x)+I$ με $\upsilon(x)=a+\beta x$, $a,\beta\in\mathbb{R}$

Οποτε $C=\{a+\beta x+I \mid a,\beta\in\mathbb{R}\}=\{\bar{a}+\bar{\beta}\bar{x} \mid a,\beta\in\mathbb{R}\}$

με $\bar{a}=a+I$, $\bar{\beta}=\beta+I$, $\bar{x}=x+I$

Μπορω να πω δηλ οτι το C ειναι ενας δ.χ διαστασης 2

πανω απο το $\mathbb{R}$

$C=\langle 1,\bar{x}\rangle=\{\bar{a}\cdot 1+\bar{\beta}\cdot\bar{x} \mid a,\beta\in\mathbb{R}\}$

οταν μας λεει οτι δ.χ διαστασης 2 σημαινει οτι

$\bar{a}+\bar{\beta}\bar{x}+\bar{a}'+\bar{\beta}'\bar{x}=(\bar{a}+\bar{a}')+(\bar{\beta}+\bar{\beta}')\bar{x}$ με την "+" ειμαι οκ, "·";

γινομενο: $\bar{a}\cdot\bar{\beta}=(a+I)(\beta+I)=a\beta+I=\overline{a\beta}$

$\bar{a}\cdot\bar{x}=(a+I)(x+I)=ax+I=\overline{ax}$

$\bar{x}\cdot\bar{x}=(x+I)(x+I)=x^2+xI+Ix+I^2=x^2+I=\bar{x}^2$

$\bar{x}^2=x^2+I$ το x^2 δεν μπορει να ειναι μεσα στο C γιατι θα ειναι

πανω απο $2^{ου}$ βαθμου, ειναι μεσα αλλα ειναι καμουφλαρισμενο

$\bar{x}^2=x^2+I=x^2+1-1+I=-1+I=-I \Rightarrow \bar{x}^2=-1$

Δεν υπαρχει πραγματικος που να ισχυει $\bar{x}^2=-1$ οποτε αυτο τωρα

το ονομαζω i (μιγαδικο)

→ Ονομαζουμε το $\bar{x}=i$ με την ιδιοτητα $i^2=-1$

Οποτε τωρα $C\to C'=\{\bar{a}+\bar{\beta}i \mid a,\beta\in\mathbb{R}\}$ και $i^2=-1$

αυτο εχει προσθεση και πολ/σμο

Θελουμε τωρα νδο $C'\cong\mathbb{C}$ σαν σωματα

Ορίζουμε λοιπόν την απεικόνιση $\psi: C' \to \mathbb{C}$ με τύπο

$\psi(\bar{a}+\bar{b}i) = a+bi$

Πρέπει να δείξω ότι ψ ομομορφ. δακτυλίων, ψ 1-1, ψ επί

"+" $\psi(\bar{a}+\bar{b}i+\bar{a}'+\bar{b}'i) = \psi((\bar{a}+\bar{a}')+(\bar{b}+\bar{b}')i) =$

$= a+a'+(b+b')i = \psi(\bar{a}+\bar{b}i)+\psi(\bar{a}'+\bar{b}'i)$

"$\cdot$" $\psi((\bar{a}+\bar{b}i)(\bar{a}'+\bar{b}'i)) = (a+I+bx+I)(a'+I+b'x+I) =$

$= aa'+aI+ab'x+aI+Ia'+I^2+Ib'x+I^2+bxa'+bxI+bxb'x+bxI+$

$+Ia'+I^2+Ib'x+I^2 = aa'+aI+ab'x+aI+ba'x+bxI+bb'x^2+$

$+bxI+I(a'+I+b'x+I) = aa'+(ab'+ba')x+bb'x^2+I =$

$= aa'+(ab'+ba')x+bb'x^2+bb'-bb'+I =$

$= aa'-bb'+(ab'+ba')x+bb'(x^2+1)+I = I$

$(aa'-bb'+(ab'+ba')x+I)$

$\bar{a}\bar{a}'-\bar{b}\bar{b}'+(\bar{a}\bar{b}'+\bar{b}\bar{a}')i \xrightarrow{\psi} aa'-bb'+(ab'+ba')i =$

$= (a+bi)(a'+b'i) = \psi(\bar{a}+\bar{b}i)+\psi(\bar{a}'+\bar{b}'i)$

μέχρι εδώ δείξαμε ότι είναι ομομορφισμός δακτυλίων

$(1,i)$ Γ.Α άρα $\bar{a}=\bar{b}=0$

$\psi(a+bi)=0 \Leftrightarrow \bar{a}+\bar{b}i=\bar{0} \Leftrightarrow \bar{a}\cdot 1+\bar{b}\cdot i=\bar{0}$ τα $(1,i)$ βάση

$\Rightarrow \bar{a}=\bar{0}=\bar{b} \Rightarrow \bar{a}+\bar{b}i=\bar{0}$ Άρα 1-1

Το επί είναι προφανές

Τελικά $\mathbb{C} \cong \mathbb{R}[x]/\langle x^2+1\rangle$

Ερώτηση: στα πεπερασμένα σώματα τι γίνεται; Δουλεύει αυτό;

7x

$\mathbb{Z}_2$ $\quad x^2+\beta x+\gamma$

αν $x=0$ οχι αναγωγο γιατι βαθμος 2

αν $x=1$ οχι αναγωγο γιατι ριζα 1

Αν $f(x)=x^2+x+1$ αναγωγο στο $\mathbb{Z}_2[x]$

$\mathbb{Z}_2[x]/\langle f(x)\rangle = I$ σωμα

$A=\{g(x)+I \mid g(x)\in \mathbb{Z}_2[x]\}$ $\quad g(x)=f(x)\pi(x)+v(x)$

$v(x)=0$ ή $\deg(v(x))=0$ ή $1 \Leftrightarrow v(x)=a+\beta x$, $a,\beta\in\mathbb{Z}_2$

$A=\{a+\beta x+I \mid a,\beta\in\mathbb{Z}_2\}=\{\bar{a}+\bar{\beta}\bar{x} \mid a,\beta\in\mathbb{Z}_2\}$

$|A|=4$ στοιχεια απο $f(x)=x^2+x+1$

A ειναι δ.χ διαστασης 2 πανω απο το $\mathbb{Z}_2$

A ειναι σωμα με 4 μονο στοιχεια

$\mathbb{Z}_2 \subseteq A=\{a+\beta\rho \mid a,\beta\in\mathbb{Z}_2,$ ρ συμβολο για το οποιο ισχυει

$\rho^2+\rho+1=0 \Rightarrow \rho^2=\rho+1\}$