$f(x) \in \mathbb{R}[x]$?	$x^2 - 2 \in \mathbb{Q}[x]$ και $\mathbb{R}[x]$ όχι ανάγωγο

$f(x) = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$

Μάθημα 22ο

20/05/16

ΛΥΣΕΙΣ ΦΥΛΛΑΔΙΟΥ 6:

1α) $r * s = 2(r+s) \not\Rightarrow$ όχι προσεταιριστική $\rightarrow$ όχι δακτύλιος

$r \boxdot s = r \cdot s$

β) $r * s = 2rs = s * r$ Αβελιανή ομάδα όχι γιατί δεν έχουμε αντίστροφο του 0.

$r \boxdot s = rs = s \boxdot r$

$\mathbb{R}^*$ $r * s$ προσεταιριστική

$\frac{1}{2} * s = \frac{1}{2} s = s$ ουδέτερο το $\frac{1}{2}$

$s^{-1} = \frac{1}{4s}$, $s^{-1} * s = 2 \cdot \frac{1}{4\cancel{s}} \cancel{s} = \frac{1}{2}$ αντίθετος

$r \boxdot s = rs$ προσεταιριστική

1 μοναδιαίο

αντίστροφο

Επιμεριστική: $(r * s) \boxdot w = r \boxdot w * s \boxdot w = (rw) * (sw) = 2rwsw$ $\not\parallel$

$(2rs) \boxdot w = 2rsw$

ΟΧΙ ΔΑΚΤΥΛΙΟΣ.

γ) $r * s = 2rs$ $r \boxdot s = r^2$	$(r \boxdot s) \boxdot w = r^2 \boxdot w = r^4$ $r \boxdot (s \boxdot w) = r \boxdot s^2 = r^2$ $\not\parallel$ ΟΧΙ ΠΡΟΣΕΤΑΙΡΙΣΤΙΚΗ $\Rightarrow$ ΟΧΙ ΔΑΚΤΥΛΙΟΣ

ΑΣΚΗΣΗ 2:

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$$

$(A,+)$ αβελιανή ομάδα

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa'-bb' & ab'+ba' \\ -ba'-ab' & -bb'+aa' \end{pmatrix} \in A$$

$(A,\cdot)$ καλά ορισμένη

$(A,\cdot)$ προσεταιριστική και, γιατί το γινόμενο των πινάκων είναι.

Μοναδιαίο: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

$$\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} aa'-bb' & a'b+b'a \\ -ab'-a'b & -bb'+aa' \end{pmatrix}$$

Αβελιανή

Αν $ab \neq 0 \Rightarrow \exists \begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

A σώμα $\xrightarrow[\cong]{\Phi} ?\ \mathbb{C}$

$\Phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a+bi$, $\quad \Phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) = \Phi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \Phi\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$

$$\Phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) = \Phi\begin{pmatrix} aa'-bb' & ab'+ba' \\ -ab'-ba' & aa'-bb' \end{pmatrix} = (aa'-bb') + (ab'+ba')i$$

$$= (a+bi)(a'+b'i) = \Phi(\quad)\Phi(\quad)$$

Φ επί προφανές

φ "1-1": $\varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \varphi\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \Rightarrow (\quad) = (\quad)$

$a+bi = a'+b'i$

ΑΣΚΗΣΗ 3:

• $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ μονάδες: $(a,\beta)(a',\beta') = (1,1) = (aa', \beta\beta') \Leftrightarrow$ a, β μονάδες του $\mathbb{Z}_3$

$a\beta \not\equiv 0 \bmod 3$

μηδενοδιαιρέτες: $(a,\beta)(a',\beta') = (0,0) = (aa', \beta\beta')$

$aa' \equiv 0 \bmod 3 \equiv \beta\beta' \Leftrightarrow a$ ή $a' = 0$, β ή $\beta' = 0$

$(a,0)$ ή $(0,\beta)$

Μηδενοδύναμα: $(a,\beta)^k = (0,0) = (a^k, \beta^k)$

$\gg$ στο $\mathbb{Z}_3$: $(a,\beta) = (0,0)$

• $\mathbb{Z}_4 \oplus \mathbb{Z}_6$: $(a,\beta)(a',\beta') = (1,1)$

$\left.\begin{array}{l} a = 1 \text{ ή } 3 \\ \beta = 1 \text{ ή } 5 \end{array}\right\}$ μονάδες

$\left.\begin{array}{ll} aa' \equiv 0 \bmod 4 & a = 0, 2 \\ \beta\beta' \equiv 0 \bmod 6 & \beta = 0, 2, 3, 4 \end{array}\right\}$ μηδενοδιαιρέτες.

π.χ. $(2,5)(2,0) = (4,0)$

$\neq (0,0)$ //

$(a,\beta)^k \equiv (0,0)$

$\left.\begin{array}{ll} a^k \equiv 0 \bmod 4 & a = 0, 2 \\ \beta^k \equiv 0 \bmod 6 & \beta = 0. \end{array}\right\}$ μηδενοδύναμο $(2,0)$ μόνο

ΑΣΚΗΣΗ 5:

$\mathbb{Z}\oplus\mathbb{Z}$ $\quad (\kappa,\lambda)$ $\quad \kappa\mathbb{Z}\oplus\lambda\mathbb{Z}$

$\mathbb{Z}$, $\kappa\mathbb{Z}$, $\kappa\in\mathbb{N}$

$\{(\nu,\nu) \mid \nu\in\mathbb{Z}\} \neq \nu(\mathbb{Z}\oplus\mathbb{Z})$

$\{(\nu,\nu) \mid \nu\in\mathbb{Z}\}$ υποομάδα $\mathbb{Z}\times\mathbb{Z}$

Ιδεώδες $(\nu,\nu)(2,3)\in\{(\mu,\nu) \mid \mu\in\mathbb{Z}\}$ όχι ιδεώδες

$\{(a,\beta) \mid a,\beta \quad\} \triangleleft \mathbb{Z}\oplus\mathbb{Z}$

υποομάδα

I πρώτο $\triangleleft\, \mathbb{Z}\oplus\mathbb{Z}$

Αν $(a,\beta)(\gamma,\delta)\in I \rightarrow (a\gamma,\beta\delta)\in I$

(a,β) ή $(\gamma,\delta)\in I$

Πρώτα ιδεώδη στο $\mathbb{Z}$: $\{0\}$, $p\mathbb{Z}$, $\mathbb{Z}$

πρώτος

$p\mathbb{Z}\oplus\mathbb{Z}$, $\mathbb{Z}\oplus p\mathbb{Z}$

$\{0\}\oplus\mathbb{Z}$ $\quad|\quad$ $p\mathbb{Z}\oplus q\mathbb{Z}$

$\mathbb{Z}\oplus\{0\}$ $\quad|\quad$ p,q πρώτοι.

Μέγιστα: $p\mathbb{Z}\oplus q\mathbb{Z} \leq \mathbb{Z}\oplus q\mathbb{Z}$

όχι μέγιστο

Μέγιστα $\mathbb{Z}\oplus q\mathbb{Z}$ ή $p\mathbb{Z}\oplus\mathbb{Z}$

$\mathbb{Z}\oplus\mathbb{Z}/I$ μέγιστο $\cong$ Σώμα

$\mathbb{Z}\oplus\mathbb{Z}/_{p\mathbb{Z}\oplus q\mathbb{Z}} \cong \mathbb{Z}_p\oplus\mathbb{Z}_q$

ΑΣΚΗΣΗ 6:

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

$\{0\}$ και $\mathbb{Z}[i]$ προφανή ιδεώδη

$\mathbb{Z}\leq\mathbb{Z}[i]$

$\mathbb{Z}\ntriangleleft\mathbb{Z}[i]$

υ μονάδα $\Rightarrow \exists \upsilon^{-1}: \upsilon\upsilon^{-1}=1$

$\upsilon\in I \Rightarrow \upsilon\cdot\upsilon^{-1}\in I \Rightarrow 1\in I$

$1\cdot a=a\in I \quad \forall a\in R$

$I=R$.

$\{bi \mid b\in\mathbb{Z}\}\ntriangleleft\mathbb{Z}[i]$

$ii=-1$.

$(2a+2bi)(2a-2bi)=8$

$8\in I \qquad 4(2+2i)\in I$

$8+8i-8\in I$

$8i\in I$

$\kappa(\mathbb{Z}+\mathbb{Z}i) \quad \kappa\in\mathbb{Z}$

$\parallel$

$\{(\kappa a+\kappa bi) \mid a,b\in\mathbb{Z}\}\triangleleft\mathbb{Z}[i]$

$\mathbb{F}$ σώμα όχι τυχαίος δακτύλιος

$f(x)\in\mathbb{F}[x]$ είναι ανάγωγο όταν δεν γράφεται: $f(x)=g(x)\cdot h(x)$ με $g(x), h(x)$ όχι σταθερά και $\deg g(x), \deg h(x)<\deg f(x)$.

Να βρούμε ανάγωγα: $\mathbb{Q}[x]$

Κριτήριο Eisenstein

$f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$

Αν $\exists p$ πρώτος με $p \mid a_i$, $i=0,\dots,n-1$

$p\nmid a_n$, $p^2\nmid a_0$. Τότε $f(x)$ ανάγωγο

ΘΕΩΡΗΜΑ: Έστω p πρώτος και $f(x)\in\mathbb{Z}[x]$. Αν $\overline{f(x)} = f(x) \bmod p$ και $\deg f(x)=\deg \overline{f(x)}$ και $\overline{f(x)}$ ανάγωγο στον $\mathbb{Z}_p[x]$, τότε και το $f(x)$ είναι ανάγωγο.

ΠΑΡΑΔΕΙΓΜΑ: $f(x)=x^3+2x+20$ είναι ανάγωγο;

$p=2 \Rightarrow p\mid 2, 20$ αλλά $p^2 \mid 20$

Άρα δεν εφαρμόζεται

Να το εξετάσουμε mod3

$\overline{f(x)}=(x^3+2x+20) \bmod 3 = \bar{1}x^3+\bar{2}x+\overline{20}$

$\bar{1}=1 \bmod 3$, $\bar{2}=2 \bmod 3$, $\overline{20}=20 \bmod 3 \equiv 2$

$\overline{f(x)}=x^3+\bar{2}x+\bar{2}\in\mathbb{Z}_3[x]$

$\deg f(x)=\deg \overline{f(x)}=3 \Rightarrow$ Αν δεν ήταν ανάγωγο θα είχε μια τουλάχιστον ρίζα: $\bar{0},\bar{1},\bar{2}$

$\overline{f}(0)=\bar{2}$, $\overline{f}(\bar{1})=\bar{2}$, $\overline{f}(\bar{2})=\bar{2}$. Άρα, $\bar{f}$ είναι ανάγωγο $\Rightarrow f$ ανάγωγο.

ΑΠΟΔΕΙΞΗ: Αν δεν ήταν ανάγωγο.

$f(x)=g(x)\cdot h(x) \Rightarrow f(x)=g(x)\, h(x) \bmod p$

$\overline{f(x)}=\overline{g(x)}\,\overline{h(x)}$ και επειδή $\deg \overline{f(x)}=\deg f(x) \Rightarrow \deg\overline{g(x)}+\deg\overline{h(x)}=\deg f(x)$

$\overline{f(x)}=\overline{g(x)}\,\overline{h(x)}$ όχι ανάγωγο ⊕ Αδύνατο ■

$\mathbb{F}$ σώμα, $\mathbb{F}[x] \trianglerighteq I$ ιδεώδες. Τότε υπάρχει πολυώνυμο $f(x)$ ώστε το $I=\{f(x)g(x) \mid g(x)\in\mathbb{F}[x]\}$

Το I γεννάται από ένα μόνο στοιχείο. Ορίζουμε $S=\{\kappa \mid \exists h(x)\in I$ και $\deg h(x)=\kappa\}$

$S\subseteq\mathbb{N}$, $0\notin S$

$0\in S \Rightarrow$ σταθερό πολυώνυμο $\in I \Rightarrow \exists a\in I$

$a\in\mathbb{F} \Rightarrow a\cdot a^{-1}=1\in I \Rightarrow I=\mathbb{F}[x]$

$S\subseteq\mathbb{N} \Rightarrow$ το S έχει ελάχιστο στοιχείο το m. Άρα υπάρχει $f(x)\in I$ με $\deg f(x)=m$.

Θα δείξουμε ότι $\forall h(x)\in I \Rightarrow h(x)=f(x)\,\pi(x)$

Με άτοπο. Αν $\exists\, h(x) \in I$ και $h(x) = f(x)\pi(x) + u(x)$ με $u(x) \neq 0 \Rightarrow h(x) - f(x)\pi(x) = u(x)$
$u(x) \in I$ με $\deg u(x) < m$. Αδύνατο

Αν I μέγιστο του $\mathbb{F}[x] \Rightarrow \mathbb{F}[x]/I$ είναι σώμα $\mathbb{F}[x]/I = \{h(x) + I \mid h(x) \in \mathbb{F}[x]\}$

Το $h(x) + I = \overline{h(x)}$ συμβολισμός

Μηδενικό (0) στο $\mathbb{F}[x]/I$ είναι το $\overline{0} = I$.

Αν $f(x) \in I \Rightarrow \overline{f(x)} = f(x) + I = I = \overline{0}$

ΕΦΑΡΜΟΓΗ: $\mathbb{R}[x]$, $x^2+1 = f(x)$ ανάγωγο.
Έστω $I = \langle f(x) \rangle = \{f(x)g(x) \mid g(x) \in \mathbb{R}[x]\}$ τότε I μέγιστο: Αν $I \subsetneq J \trianglelefteq \mathbb{R}[x] \Rightarrow$
$\Rightarrow J = \langle k(x) \rangle$ κάποιο πολυώνυμο
Άρα, $f(x) \in J \Rightarrow f(x) = k(x)\pi(x)$ και επειδή $I \subsetneq J \Rightarrow \deg f(x) > \deg k(x) \Rightarrow f(x)$ όχι ανάγωγο
Αδύνατο

$I = \langle f(x) \rangle$ μέγιστο $\Rightarrow \mathbb{R}[x]/I =$ σώμα

$\mathbb{R}[x]/I = \mathbb{R}[x]/\langle x^2+1 \rangle = \{g(x) + \langle x^2+1 \rangle \mid g(x) \in \mathbb{R}[x]\}$.

$\deg g(x) \geq 2 \Rightarrow g(x) = f(x)\pi(x) + u(x)$
$u(x) = 0 \Rightarrow g(x)$ πολλαπλάσιο του $f(x) \Rightarrow g(x) + I = I \Rightarrow \overline{g(x)} = \overline{0}$
$u(x) \neq 0 \Rightarrow \deg u(x) < 2 \Rightarrow \boxed{u(x) = ax + b \mid a, b \in \mathbb{R}}$
$g(x) = f(x)\pi(x) + u(x) \Rightarrow \overline{g(x)} = f(x)\pi(x) + u(x) + I = u(x) + I = \overline{u(x)}$

Παρατηρήσεις: Ονομάζουμε $\mathbb{C} = \mathbb{R}[x]/\langle x^2+1 \rangle = \{\overline{ax+b} \mid a, b \in \mathbb{R}\} = \{\overline{a}\,\overline{x} + \overline{b} \mid a, b \in \mathbb{R}\}$
$\overline{a} = a + I$. Συνήθως γράφουμε $\overline{a} = a$. Δηλαδή, θεωρούμε ότι το $\mathbb{R}$ "ζει" μέσα στο $\mathbb{C}$.
$\overline{x^2+1} = x^2 + 1 + I = (x+I)(x+I) + 1 + I = \overline{x}\cdot\overline{x} + \overline{1} = (\overline{x})^2 + 1 = \overline{0}$

Αν ονομάσουμε το $\overline{x} = i$
$\mathbb{C} = \{a\overline{x} + b = ai + b \mid a, b \in \mathbb{R}\}$