19/5/17 Μαθημα 19ο

#7 1) $(\mathbb{R}, *, \boxdot)$ $r*s = 2(r+s)$ $r \boxdot s = rs$

$(r*s)*t = (2(r+s))*t = 2(2(r+s)+t)$

$r*(s*t) = r*(2(s+t)) = 2(r+2(s+t))$ $\neq$ Δεν είναι

2) $r*s = 2rs$ $r \boxdot s = rs$

Δεν ορίζεται ο αντιστροφος-αντιθετος για καμια πραξη.
Αρα δεν είναι.

Το $(\mathbb{R}^*, \boxdot)$ αβελιανη ομαδα.

Αν η $*$ είναι προσεταιριστική και αν ισχυει η επιμεριστική

$(r*s)*t = (2rs)*t = 2(2rs)t = 4rst$

$r*(s*t) = r*(2st) = 2r(2st)$

Επιμεριστικη:

$r*(s \boxdot t) = r*s \boxdot r*t$

$r*(st) = 2rst$ (+)

$r*s \boxdot r*t = 2rs \boxdot 2rt = (2rs)(2rt) = 4r^2st \neq$ (+)

Δεν ειναι απε με αυτη την επιλογη

$r*s = 2rs$ $r \boxdot s = r^2$ στο $\mathbb{R}^*$

$(\mathbb{R}^*, *)$ αβελιανη ομαδα;;;

Προσεταιριστικη ισχυει, αβελιανη είναι.

Ουδετερο-μοναδιαιο: $r*e = r = e*r$ $e = ;$

$r*e = r \Rightarrow 2re = r \overset{r\neq 0}{\Rightarrow} e = \frac{1}{2}$.

Αντιθετος - Αντιστροφος: $\forall r \ \exists r'$ ωστε $r*r' = e = r'*r$

$r*r' = \frac{1}{2} \Rightarrow 2rr' = \frac{1}{2} \Rightarrow r' = \frac{1}{4r}$

Προσεταιριστικη $\boxdot$

$(r \boxdot s) \boxdot t = r^2 \boxdot t = r^4$ $\neq$ Δεν είναι

$r \boxdot (s \boxdot t) = r \boxdot s^2 = r^2$

2) $A = \left\{ \begin{pmatrix} \alpha & b \\ -b & a \end{pmatrix}, a, b \in \mathbb{R} \right\}$ με προσθεση κ πολ/σμο πινακ

Πραξει καλα ορισμενες :

$$\begin{pmatrix} \alpha & b \\ -b & \alpha \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & \alpha' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ -b-b' & a+a' \end{pmatrix}$$

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

Προσθεση, πολ/σμος πινακων προσεταιριστικές.

$(A,+)$ αβελιανή ομαδα $\Rightarrow$ Η επιμεριστική ισχύει απο τους πινακες $\Rightarrow$ A δακτυλιος

Για $b=0$ και $\alpha=1 \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow$ A μοναδιαιος

Για A με $\det A \neq 0$ εξετάζουμε αν υπαρχει αντιστροφ

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} \frac{a}{\det A} & -\frac{b}{\det A} \\ \frac{b}{\det A} & \frac{a}{\det A} \end{pmatrix}$$

Μπορουμε να ορίσουμε:

Ισομορφισμό $\phi : A \to \mathbb{C}$ με τυπο $\phi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+bi$

Η ϕ είναι ομομορφισμός δακτυλ. :

$$\phi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \right) = \phi\left(\begin{pmatrix} a+a' & b+b' \end{pmatrix} \right)$$

δηλ. $a+a'+i(b+b')$

$$\phi\left[\begin{pmatrix} \alpha & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \right] = \phi \begin{pmatrix} aa'-bb' & ab'+ba' \\ -ab'-ba' & aa'-bb' \end{pmatrix} =$$

$= aa' - bb' + i(ab' + ba') = \Phi(\quad)\,\Phi(\quad)$

1-1 $\Phi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \Phi\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \Rightarrow a + ib = a' + ib' \Leftrightarrow$

$a = a'$

$b = b'$

Επι προφανές.

3) $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Έχει 9 στοιχεία

Αν $A, B \leq \mathbb{Z}_3$ τότε $A \times B \leq \mathbb{Z}_3 \times \mathbb{Z}_3$

$\to$ 4 υποομάδες

$\{(1,1) \to (2,2) \to (0,0)\}$ κυκλική τάξη 3

$\{(1,2) \to (2,1) \to (0,0)\}$ Αφού είναι υποομάδα θα πρέπει να διαιρεί την τάξη της ομάδας.

Μονάδες: $(a,b)(a',b') = (1,1)$

άρα έχουμε $(aa', bb') = (1,1)$

$aa' = 1 \Leftrightarrow (a,3) = 1 \Leftrightarrow a = 1, 2 = b$.

Άρα 4 μονάδες

Μηδενοδιαιρέτες: $(a,b) \neq (0,0)$ & $(a',b') \neq (0,0) \Rightarrow$

$\Rightarrow (a,b)(a',b') = (0,0)$

$\Rightarrow aa' = 0 = bb'$

Μηδενοδιαιρέτες στο $\mathbb{Z}_3$

Το ίδιο και για το b.

$\boxed{\text{Σώμα μόνο το 0}}$

$(a,0)$ με $a \neq 0$

$(0,b)$ με $b \neq 0$

$\}$ 4 μηδενοδιαιρέτες

Μηδενοδυναμα: $(a,b)\neq(0,0)$ ι $(a,b)^k=(0,0)$
αρα $a^k=0=b^k$ στο $\mathbb{Z}_3$ δεν εχει τετοια στοιχεια

· $\mathbb{Z}_4 \oplus \mathbb{Z}_6$
Μοναδες $(a,b)(a',b')=(1,1)$
$aa'=1_4$ $\quad bb'=1_6$
$a=1,3$ $\quad b=1,5$
$(1,1)$, $(1,5)$, $(3,1)$, $(3,5)$
Μηδενοδιαιρετες: $(\alpha,0)$ ή $(0,b)$
$\alpha\neq 0$ $\quad b\neq 0$
(a,b) με b μηδενοδιαιρετη στο $\mathbb{Z}_6$.

$\mathbb{Z}_4 : 2$
$\mathbb{Z}_6 : 2,3,4$

$(\alpha,2)\quad(0,3)=(0,0)$
α: τυχαιο
$(2,b)(2,0)=(0,0)$
b: τυχαιο
$(a,3)$, $(a,4)$

Μηδενοδυναμα: $(a^k,b^k)=(0,0)$
$a^k=0_4$, $b^k=0_6$
$a=2$ στο $\mathbb{Z}_4$
$b=0$
$4\to16\equiv4$, $2\to4\to8\equiv2$, $3\to9\to3$
$(2,0)$ μηδενοδυναμο

4) R μοναδιαιος δακτυλιος
$U=\{r\in R$ με r μοναδα$\}$ ομαδα
$U\neq\emptyset$ $1\in U$
πραξη κλειστη. Αν $r,r'\in U \Rightarrow rr'\in U \Leftrightarrow \exists$ αντιστροφος
$((r')^{-1}r^{-1})\cdot(rr')=1=(rr')((r')^{-1}r^{-1})$
Προσεταιριστικη ειναι απο τον R.
$1\in U$ και για καθε στοιχειο υπαρχει ο αντιστροφος,

$\mathbb{Z}_4 \oplus \mathbb{Z}_6 \Rightarrow U = \{(1,1), (1,5), (3,1) (3,5)\}$
$(3,5) \to (1,1)$ $\cong$ $\mathbb{Z}_2 \times \mathbb{Z}_2$

5) $\mathbb{Z} \oplus \mathbb{Z}$

Ιδεωδη $\mathbb{Z} \to k\mathbb{Z}$, $k \in \mathbb{N}$

Υποομαδες $\mathbb{Z} \times \mathbb{Z}$

$k\mathbb{Z} \times m\mathbb{Z}$, με $k, m \in \mathbb{N}$

Ειναι $k\mathbb{Z} \oplus m\mathbb{Z}$ υποδακτυλιος

$(ka, mb)(\gamma, \delta) = (ka\gamma, mb\delta) \in k\mathbb{Z} \oplus m\mathbb{Z}$

Αρα είναι υποδακτυλιοι

Δηλαδη εξεταζουμε τις δυο ιδιοτητες: $(a,b) + (a',b')$ &
$(a,b)\cdot(a',b')$

Στα ιδεωδη πρεπει να ισχυει η ιδιοτητα:

$\forall (a,b) \in k\mathbb{Z} \oplus m\mathbb{Z}$ και
" (ka', mb')

$\forall (\gamma, \delta) \in \mathbb{Z} \oplus \mathbb{Z}$ πρεπει

$(\alpha, b)(\gamma, \delta) = (\gamma, \delta)(\alpha, b) \in k\mathbb{Z} \oplus m\mathbb{Z}$

$(k\alpha', mb')(\gamma, \delta) = (ka'\gamma, mb'\delta) \in k\mathbb{Z} \oplus m\mathbb{Z}$

Μεγιστα ιδεωδη του $\mathbb{Z}$ είναι $p\mathbb{Z}$, p πρωτος

$p\mathbb{Z} \oplus q\mathbb{Z}$ είναι μεγιστο???

$3\mathbb{Z} \oplus 2\mathbb{Z} \subsetneq 3\mathbb{Z} \oplus \mathbb{Z}$ ή $\mathbb{Z} \oplus 2\mathbb{Z}$

Αυτά που είναι $p\mathbb{Z} \oplus \mathbb{Z}$ ή $\mathbb{Z} \oplus p\mathbb{Z}$ είναι μεγιστα?

$\mathbb{Z} \oplus p\mathbb{Z} \subsetneq \mathbb{Z} \oplus k\mathbb{Z} \Rightarrow k \mid p \Rightarrow k = 1$

Αρα $\mathbb{Z} \oplus p\mathbb{Z} \subsetneq \mathbb{Z} \oplus \mathbb{Z} \Rightarrow \mathbb{Z} \oplus p\mathbb{Z}$ ή $p\mathbb{Z} \oplus \mathbb{Z}$ μεγιστο

Πρωτα ιδεωδη του $\mathbb{Z}$: $\{0\}$ και $p\mathbb{Z}$

$\mathbb{Z}$ ακεραια περιοχή: $I \trianglelefteq \mathbb{Z}$ πρωτο $\Leftrightarrow \mathbb{Z}/I$ ακεραια περιοχή

$I = kZ \Rightarrow Z/I = Z/kZ \cong Z_k$ ακέραια περιοχή $\Leftrightarrow$
$k = 0$ ή k = πρώτος
Πρώτα στον $Z \oplus Z$
$\{0\} \oplus pZ$ $(a,b)(c,d) = (ac, bd) \in \{0\} \oplus pZ$
$pZ \oplus \{0\}$
$(a,b)(c,d) \in I \oplus J \Rightarrow$
(a,b) ή $(c,d) \in I \oplus J$
$ac = 0$ και $bd \in pZ$
$ac = 0$ και $bd = pn$
$a = 0$ και $p \mid b$ ή d
Αν $a = 0$ και $p \nmid b$ αλλά $p \mid d$ και $c \neq 0$
$(0,b)$ και (c, pd')
Άρα $\{0\} \oplus pZ$ όχι πρώτος
$\{0\} \oplus \{0\}$ όχι
$(0,6)(6,0) = (0,0)$ αλλά
$(0,6), (6,0) \notin \{0\} \oplus \{0\}$
$pZ \oplus qZ$ όχι
$p = 2$, $q = 3$
$(2,2)(3,3) = (6,6) \in 2Z \oplus 3Z$
$(2,2) \notin 2Z \oplus 3Z$
$(3,3) \notin 2Z \oplus 3Z$
$Z \oplus 2Z \ni (a,b)(c,d)$ $ac \in Z$ ισχύει
$(1,2)$ $bd \in 2Z \Rightarrow$
$2 \mid b$ ή d
Για $2 \mid b \rightarrow (a,b) \in Z \oplus 2Z$
$Z \oplus pZ$ και $pZ \oplus Z$, $Z \oplus Z$

Αλγόριθμοι διαίρεσης

F σώμα τα F[x] δακτύλιοι πολυωνύμων. Αν $f(x)$, $g(x) \in F[x]$ τότε $\exists!$ $\pi(x), u(x) \in F[x]$ ώστε
1) $f(x) = \pi(x) g(x) + u(x)$
2) $u(x) = 0$ ή $\deg u < \deg g$

Πρόταση: Αν $f(x) \in F[x]$ τότε το $a \in F$ είναι ρίζα του $f(x)$ ($f(\alpha)=0$) ανν το $x-a$ διαιρεί το $f(x)$.

Αν το $x-a$ διαιρεί το $f(x) \Leftrightarrow f(x) = \pi(x)(x-a)$. Τότε
$f(\alpha) = \pi(a)(\alpha-\alpha) = \pi(\alpha)\cdot 0 = 0 \Rightarrow a$ ρίζα του $f(x)$

Αν το α είναι ρίζα του $f(x)$ τότε $f(\alpha)=0$

Από τον αλγόριθμο της διαίρεσης: $f(x) = \pi(x)(x-a) + u(x)$
με $u(x) = 0$ ή $\deg u(x) < \deg(x-a)$
Αν $u(x) = 0 \Rightarrow x-a \mid f(x)$
Αν $u(x) \neq 0 \Rightarrow \deg u(x) < 1 \Rightarrow \deg u(x) = 0 \Rightarrow u(x) = c$ σταθερό
Τότε $f(x) = \pi(x)(x-a) + c$
$f(\alpha) = \pi(\alpha) 0 + c \Rightarrow 0 = c$.

Πρόταση: Έστω F σώμα και $f(x) \in F[x]$ με $\deg f(x) = n$. Τότε το $f(x)$ έχει το πολύ n διακεκριμένες ρίζες.
απόδειξη:
Θα το δείξουμε με επαγωγή:
$n=0 \Rightarrow f(x) = c$ έχει μηδέν ρίζες
$n=1 \Rightarrow f(x) = ax+b$ έχει μια ρίζα.
Υποθέτουμε ότι η πρόταση ισχύει για όλα τα πολυώνυμα βαθμού $<n$.
Έστω ότι η $f(x)$ έχει τουλάχιστον $n+1$ διακεκριμένες ρίζες $\{\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1}\}$
Τότε το $f(x)$ διαιρείται από το $x-a_1$
$f(x) = (x-a_1) h(x)$ με $\deg h(x) < n$.

$h(x)$ έχει n διακεκριμένες ρίζες
$f(\alpha_i) = (\alpha_i - \alpha_1)\, h(\alpha_i)$ με $i \neq 1$.
Άρα $h(\alpha_i) = 0$ $i = 2, \dots, n+1$
Από την επαγωγική υπόθεση αυτό είναι άτοπο.

Πρόταση: Έστω F άπειρο σώμα και $f(x) \in F[x]$ το οποίο έχει άπειρες ρίζες. Τότε $f(x) = 0$.
Απόδειξη:
Αν $f(x) = 0$ τότε $f(\alpha) = 0$ $\forall \alpha \in F$ (άπειρο)
Αν $\deg f(x) = n$, από το προηγούμενο έχει το πολύ n διακεκριμένες ρίζες. Αλλά η υπόθεση δηλώνει ότι έχει άπειρες. Αδύνατο.
Άρα $\deg f(x)$ δεν υπάρχει $\Leftrightarrow f(x) = 0$.

Πόρισμα: Αν F σώμα και $f(x), g(x) \in F[x]$ με $f(\alpha) = g(\alpha)$ για άπειρο πλήθος στοιχείων $\alpha \in F$ τότε $f(x) = g(x)$.

π.χ. $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ και $f(x) = x^2 + x \in R[x]$.
όχι έτσι
αλλά γράφεται $f(x) = (1,1)x^2 + (1,1)x$.
$\deg f = 2$.
$f(\alpha, b) = (1,1)(\alpha, b)^2 + (1,1)(\alpha, b) = (1,1)(a^2, b^2) + (1,1)(\alpha, b)$
$= (\alpha^2, b^2) + (a, b) = (a^2 + a, b^2 + b)$.

βάζω το (α, b) στη θέση του x.
η $\alpha, b = 0$ ή 1
$f(1,1) = (0,0) = f(1,0) = f(0,1) = f(0,0)$
έχει 4 ρίζες βαθμού 2. τότε τι συμβαίνει με την θεωρία??
Συμβαίνει αυτό γιατί δεν είμαστε σε σώμα

π.χ. $x^2+1 \in \mathbb{R}[x]$ δεν έχει καμία ρίζα

Ορισμός: Ένα πολυώνυμο $f(x) \in F[x]$ με F σώμα και $\deg f \geq 1$ θα καλείται <u>ανάγωγο</u> αν <u>δεν</u> γράφεται σαν γινόμενο πολυωνύμων μικρότερων βαθμών.

π.χ. $f(x) = 3x + 2 = 3\left(x + \frac{2}{3}\right)$ δεν το δεχόμαι.