Μάθημα 21ο

17/05/16

ΛΥΣΕΙΣ ΦΥΛΛΑΔΙΟΥ 5:

ΑΣΚΗΣΗ 3

$|G| = p \cdot q$, p, q πρώτοι, $p \neq q$ ⊕
$\exists!\ H \leq G$, $|H| = p$, $\exists!\ K \leq G$, $|K| = q$

α) $H \cap K = \{1\}$
$a \in H \cap K \Rightarrow O(a) | p, q$ ⊕ $\Rightarrow O(a) = 1$, $a = 1$

β) $H \triangleleft G$ | $G = HK \Leftrightarrow \forall g \in G\ \exists h \in H$ και $k \in K$ με $g = hk$

$HK \leq G$

$O(g) | p \cdot q \Rightarrow O(g) = 1$
$O(g) = p \Rightarrow |\langle g \rangle| = p$ και H μοναδική $\Rightarrow g \in H$
$O(g) = q \Rightarrow g \in K$
$O(g) = p \cdot q \rightarrow G = \langle g \rangle$

H και K κυκλικές
$H = \langle h \rangle$ και $K = \langle k \rangle$
$O(hk)$ Αν G Αβελιανή $\Rightarrow O(hk) = [O(h) \cdot O(k)]$ ΕΚΠ $= p \cdot q$

$1, p, q, p \cdot q$
$O(hk) = 1 \Rightarrow hk = 1 \Rightarrow h = k^{-1}$ με $O(h) = p$ και $O(k) = q$!

$O(hk) = p \Rightarrow hk \in H \Rightarrow k \in H$!
και το q απορρίπτεται
Άρα $O(hk) = p \cdot q \Rightarrow G$ κυκλική
$G \cong \mathbb{Z}_{pq}$ οπότε $H \cong q\mathbb{Z}_{pq}$ και $K \cong p\mathbb{Z}_{pq}$

$H, K \trianglelefteq G$ αφού G κυκλική
$hk = kh$ αφού G αβελιανή

ΑΣΚΗΣΗ 4:

G αβελιανή, $|G| = 100 = 2^2 \cdot 5^2$
Διαμερίσεις του 2: 2, $1+1$
Υπάρχουν 2 2 μη-ισόμορφες
$2 \quad 2 \rightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{100}$
$2 \quad 1+1 \rightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20} \times \mathbb{Z}_5$
$1+1 \quad 2 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_{2} \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_{50}$
$1+1 \quad 1+1 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10} \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_5$

ΑΣΚΗΣΗ 5:

$\mathbb{Z}_{36}$
$\langle 18 \rangle = \{18, 0\} \cong \mathbb{Z}_2 \leq \mathbb{Z}_{36}$
$\langle 36 \rangle = \langle 0 \rangle = \{0\}$

$$\mathbb{Z}_{36}/\langle 18 \rangle = \mathbb{Z}_{36}/18\cdot\mathbb{Z}_{36} = \mathbb{Z}/36\mathbb{Z} \Big/ 18\mathbb{Z}/36\mathbb{Z} \cong \mathbb{Z}/18\mathbb{Z} = \mathbb{Z}_{18}$$

$\mathbb{Z}_{36} = \mathbb{Z}/36\mathbb{Z}$

$$\langle 18 \rangle / \langle 36 \rangle = {}^{18\mathbb{Z}_{36}}/_{0\mathbb{Z}_{36}} = \left(18\mathbb{Z}/36\mathbb{Z}\right) \Big/ \left(0\mathbb{Z}/36\mathbb{Z}\right) \cong \mathbb{Z}_2$$

$$\left(\mathbb{Z}_{36}/18\mathbb{Z}_{36}\right)/\left(18\mathbb{Z}_{36}/0\right) \cong \mathbb{Z}_2 \cong 9\mathbb{Z}_{18}$$

$$\left(\mathbb{Z}_{36}/18\mathbb{Z}_{36}\right)/\left(18\mathbb{Z}_{36}/\langle 0\rangle\right) \cong \mathbb{Z}_{18}/9\mathbb{Z}_{18} \cong \mathbb{Z}_9$$

R δακτύλιος $\longrightarrow$ R[x] πολυωνυμικός δακτύλιος

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n + 0x^{n+1} + \cdots \mid a_i \in R,\ a_n \neq 0\}$$

$0 \cdot x$ = μηδενικό πολυώνυμο $= 0$

Αν ο R έχει μοναδιαίο $1 \to 1 \cdot x^\kappa = x^\kappa$

$a_0 + a_1x + \cdots = b_0 + b_1x + \cdots$

$a_i = b_i,\ \forall i \in \mathbb{N}$

$(a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = c_0 + c_1x + \cdots$

$c_i = a_i + b_i$

$(a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = c_0' + c_1'x + \cdots$

$c_i' = \sum_{\kappa=0}^{i} a_\kappa b_{i-\kappa}$

$\deg(a_0 + a_1x + \cdots) = n$ <u>αν</u> $a_n \neq 0$ και $a_\kappa = 0,\ \forall \kappa > n$

$0 \cdot x$ δεν έχει βαθμό.

$\deg(f(x)+g(x)) \leq \max(\deg f(x), \deg g(x))$

Αν R ακέραια περιοχή τότε $\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x),\ f(x)\,g(x) \neq 0$

ΠΡΟΣΟΧΗ: Στον R. Το αν έχει ή όχι ρίζα το f(x) εξαρτάται από τον R.

Ευκλείδεια διαίρεση $R=\mathbb{F}$ σώμα

$\forall f(x), g(x) \in \mathbb{F}[x]$, $\exists! \pi(x), \upsilon(x) \in \mathbb{F}[x]$ με $f(x)=g(x)\pi(x)+\upsilon(x)$

$\upsilon(x)=0$ ή $\deg \upsilon(x) < \deg g(x)$

Ρίζα a είναι ρίζα του $f(x)$ <u>αν</u> $f(a)=0 \Leftrightarrow f(x)=(x-a)\pi(x)$

ΟΡΙΣΜΟΣ: Έστω $\mathbb{F}$ σώμα και $f(x) \in \mathbb{F}[x]$ με $\deg f(x) \geq 1$. Το $f(x)$ καλείται **ανάγωγο** στον $\mathbb{F}[x]$, αν δεν υπάρχουν πολυώνυμα $g(x)$ και $h(x)$ μικρότερου βαθμού, ώστε $f(x)=g(x)h(x)$

ΘΕΩΡΗΜΑ: Έστω $\mathbb{F}$ σώμα και $f(x)$ πολυώνυμο βαθμού ≥ 1. Τότε το $f(x)$ γράφεται σαν γινόμενο αναγώγων. Δηλαδή υπάρχουν ανάγωγα πολυώνυμα $f_1(x), \dots, f_u(x)$

$f(x)=f_1(x) \dots f_u(x)$.

Επαγωγή στον $\deg f(x)$

Αν $f(x)=ax+b$ τότε είναι ανάγωγο. Υποθέτουμε ότι ισχύει για όλα τα πολυώνυμα βαθμού $<n$. Έστω $\deg f(x)=n$.

Αν $f(x)$ ανάγωγο, τότε η πρόταση ισχύει.

Αν $f(x)$ δεν είναι ανάγωγο, υπάρχουν πολυώνυμα $g(x)$ και $h(x)$ με $f(x)=g(x)\cdot h(x)$

Εδώ $\deg g(x), \deg h(x) < n$.

Εφαρμόζεται η πρόταση. Άρα, υπάρχουν ανάγωγα $g_1(x), \dots, g_u(x)$ και $h_1(x), \dots, h_e(x)$

$g(x)=g_1(x) \cdots g_u(x)$, $h(x)=h_1(x) \cdots h_e(x)$

$f(x)=g_1(x) \cdots g_u(x) h_1(x) \cdots h_e(x)$

ΠΑΡΑΔΕΙΓΜΑ: $\mathbb{F}=\mathbb{Z}_3$, $f(x)=x^3+2x^2+2x+1 \in \mathbb{Z}_3[x]$

$= x^3-1x^2-x+1$.

$f(1)=1^3+2\cdot 1^2+2\cdot 1+1=0+0=0$

$f(x)=(x-1)(x^2+2)=(x+2)(x^2+2)$

$g(x)=x^2+2$, $g(1)=0 \Rightarrow g(x)=(x-1)(x+1)$

$g(x)=(x-1)(x-2)=(x+2)(x+1)$

$h(x)=x^3+2x+1$ Ανάγωγο

Ανάγωγα στον $\mathbb{Q}[x]$

$f(x) \in \mathbb{Q}[x] \Leftrightarrow f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$a_i \in \mathbb{Q} \Leftrightarrow a_i = \frac{q_i}{r_i} \in \mathbb{Q}$

$f(x) = \frac{q_0}{r_0} + \frac{q_1}{r_1} x + \cdots + \frac{q_n}{r_n} x^n$

Αν $r = \text{ΕΚΠ}[r_0, r_1, \ldots, r_n]$

$r f(x) = q_0' + q_1' x + \cdots + q_n' x, \quad q_i' \in \mathbb{Z}$

ΘΕΩΡΗΜΑ: Έστω $f(x) \in \mathbb{Z}[x]$. Αν το $f(x)$ γράφεται σαν γινόμενο αναγώγων στον $\mathbb{Q}[x]$, τότε μπορεί να γραφεί σαν γινόμενο αναγώγων και στον $\mathbb{Z}[x]$.

Wanted

Κριτήριο Eisenstein: Έστω $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Αν p πρώτος ώστε $p \mid a_0, a_1, \ldots, a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Τότε το $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x] \geq \mathbb{Z}[x]$.

ΕΦΑΡΜΟΓΕΣ:

1) $f(x) = 2x^5 + 9x^4 + 3x^2 + 15x + 12$. Εξετάστε αν είναι ανάγωγο στον $\mathbb{Q}[x]$.

$3 \mid 12, 15, 3, 9$
$3 \nmid 2$ και $3^2 \nmid 12$
} Από Eisenstein $f(x)$ ανάγωγο

2) $x^2 - 2 \in \mathbb{Q}[x]$

$p = 2 \mid a_0$, $p = 2 \mid a_2 = 1$, $p^2 = 4 \nmid 2 \Rightarrow$ Ανάγωγο.

3) $f(x) = x^4 + 1$, Δεν χρησιμοποιείται το Κριτήριο Einstein.
Αν δεν ήταν ανάγωγο $f(x) = g(x) \cdot h(x)$.
$f(x+1) = g(x+1) h(x+1)$
$f(x+1) = (x+1)^4 + 1 = x^4 + \binom{4}{1} x^3 \cdot 1 + \binom{4}{2} x^2 1^2 + \binom{4}{3} x 1^3 + 1^4 + 1$

$x^4 + 4x^3 + 6x^2 + 4x + 2 \rightarrow$ Ανάγωγο για $p = 2$ Αδύνατον.
Άρα, $f(x)$ ανάγωγο.