$\dots, n = p_1 \cdot \ldots \cdot p_t$

15.03.2018

Algebră
- curs 4 -

K corp comutativ. Inelul de polinoame $K[X]$

Prop. $J \trianglelefteq K[X] \Rightarrow \exists f \in K[X]$ a.î. $J = f \cdot K[X] = \{f \cdot g \mid g \in K[X]\}$

Analogia $K[X] \mapsto \mathbb{Z}$

Th. împ cu rest. numere întregi

$a, b \in \mathbb{Z}, b \neq 0, \Rightarrow \exists q, r \in \mathbb{Z}$ a.î. $a = b \cdot q + r, 0 \leq r < |b|$

Th. împ. cu rest polinoame

$f, g \in K[X], g \neq 0 \Rightarrow \exists q, r \in K[X]$ a.î. $f = g \cdot q + r$, grad r < grad g

În $\mathbb{Z}$: $\forall n \in \mathbb{Z}, n \neq 0, n \neq \pm 1$ se scrie $n = \pm p_1^{a_1} \ldots p_r^{a_r}$, p_j - prim $\forall j = \overline{1, r}$

Scrierea e unică, dar ordinea factorilor nu.

Teorema fundamentală a aritmeticii

Def $f \in K[X]$, grad $f \geq 1$ se numește ireductibil dacă f nu se poate scrie $f = g \cdot h$, $g, h \in K[X]$ și grad $g <$ grad f, grad $h <$ grad f.

polinomul ireductibil $\longmapsto$ nr prim din $\mathbb{N}$

Analogul th. fundamentale a aritmeticii pt $K[X]$

$\forall f \in K[X]$, $f \neq 0$, grad $f \geq 1$ se scrie „unic" ca produs de polinoame ireductibile.

Ce înțeleg prin „unic"? $f = f_1 \cdot f_2 \cdot \ldots \cdot f_r$, $f_j \in K[X]$ ireductibile
$= (k f_1)(\frac{1}{k} f_2) \cdot f_3$

Obs. 1. $U(\mathbb{Z}) = \{\pm 1\}$

Obs 2. $U(K[\mathbb{Z}]) = \{k \in K^*\}$

Dem obs. 2. „$\supseteq$" $k \cdot k^{-1} = 1$

„$\subseteq$" Fie $F \in U(K[\mathbb{Z}]) \Rightarrow \exists g \in K[X]$ a.î. $f \cdot g = 1$. $\Rightarrow$ grad f + grad $g = 0$ $\Rightarrow$ grad g = grad $f = 0$, $f \in K^*$

Contraexemplu: $\mathbb{Z}_{100}[X]$ $(\overline{3} + \overline{10}x)(\overline{a} + \overline{b}x) = \overline{1}$

$$\left.\begin{array}{l} \overline{3} \cdot \overline{a} = \overline{1} \\ 33 \cdot 3 = -1 \\ (-33) \cdot 3 = 1 \end{array}\right| \begin{array}{l} \overline{10} \cdot \overline{b} = \overline{0}, \ b = 10k, k \in \mathbb{Z} \\ \Rightarrow \quad a = 67 \end{array}$$

$\overline{3}\overline{b} + \overline{10}\,\overline{a} = \overline{0}$ $\qquad \overline{30}k + \overline{670} = \overline{0} \Rightarrow \overline{30}k = \overline{30}$

Aleg $k = 1$ $\qquad 100 \mid 30(k-1) \Rightarrow 10 \mid k-1$

Adaos: $\left.\begin{array}{l} f \in K[X] \\ \text{grad } f \geq 1 \end{array}\right| \Rightarrow f$ se scrie unic

$f = k\, f_1 \cdot f_2 \cdot \ldots \cdot f_r$, $k \in \mathbb{N}^*$

f_j ireductibil și monic, $\forall j = \overline{1,r}$

Ex: $(R,+,\cdot)$ inel comutativ, $u \in U(R)$

x nilpotent asta ce înseamnă că

$\exists\, n \in \mathbb{N}^*$ a.î. $x^n = 0$. Arătați că $u+x \in U(R)$

$$u^n = u^n - x^n = (u-x)(u^{n-1} + u^{n-2}x + \dots + u x^{n-2} + x^{n-1})$$

$(-x)^n = 0$ (din faptul că $x^n = 0$)

$$u^n - (-x)^n = (u+x)(\dots\dots\dots\dots)$$

$\Rightarrow u+x$ inversabil

singuratic - monarh

$g \in K[X]$ se numește monic dacă

$$g(x) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$$

O altă analogie CMMDC

$\mathbb{Z}$, $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$ ptr că 0 divide orice nr natural. $d(a,b)$ e cel mai mare divizor comun al numerelor a și b.

$$d \in \mathbb{N}^* \begin{cases} d \mid a \text{ și} \\ d \mid b \\ \forall e \in \mathbb{Z},\ e \mid a \text{ și } e \mid b \Rightarrow e \mid d. \end{cases}$$

$K[X]$ $f, g \in K[X]$ nu ambele 0.

$h = (f, h)$ = c.m.m.d.c al polinoamelor f, g

$K[X]$ monic

$$\begin{cases} h \mid f \\ h \mid g \\ \text{dacă } h_1 \mid g \text{ și } h_1 \mid f \Rightarrow h_1 \mid h. \end{cases}$$

T: $\exists$ c.m.m.d.c pentru f, g și se calculează după aceeași regulă ca în $\mathbb{Z}$.

$f = k_1 \cdot f_1^{a_1} \cdot f_2^{a_2} \cdots f_r^{a_r}$, f_j - ireductibile monice, $f_i \neq f_j$ pt $i \neq j$

$g = k_2 \, g_1^{b_1} \cdot g_2^{b_2} \cdots g_s^{b_s}$, g_j - ireductibile monice

$k_1 \in K^*$, $a_j \in \mathbb{N}^*$, $\forall j = \overline{1,r}$

$b_j \in \mathbb{N}^*$, $\forall j = \overline{1,s}$ $\quad g_i \neq g_j$ pt $i \neq j$

$\boxed{(f, g) = \prod \text{(factori ireductibili comuni la puterea cea mai mare)}}$

Dacă nu există factori ireductibili comuni pentru $f, g \Rightarrow (f, g) = 1$.

$(21, 36) = 3$.

$m, n \in \mathbb{Z}$

$3 = 21m + 36n \Rightarrow 1 = 7m + 12n \Rightarrow 1 = 7 \cdot (-5) + 12 \cdot 3$

$3 = 21(-5) + 36 \cdot 3$

Teoremă $\forall a, b \in \mathbb{Z}$ $(a, b) \neq (0, 0)$

$\exists\, m, n \in \mathbb{Z}$ a.î. $am + bn = (a, b)$

Dem bazată pe th. împărțirii cu rest.

Analog ptr polinoame $K[X]$, $f, g \in K[X]$, $h = (f, g)$

$\exists\, f_1, g_1 \in K[X]$ a.î. $f \cdot f_1 + g \cdot g_1 = (f, g)$

Algoritmul RHO al lui Pollard nu e examen

RSA $n = p \cdot q$. Scop $n \in \mathbb{N}$ număr compus și vrem să găsim factori netriviali

$f \in \mathbb{Z}[X]$, grad $f = 2$. Aici se folosește $f(x) = x^2 + 1$

Alegem $x_0 \in \mathbb{Z}$ arbitrar. $x_{n+1} = f(x_n) \pmod{n}$ $\forall n$