

Algebra - 1

Def (inel) $(R, +, \cdot)$ R mult, $+$ și - sunt operații R
 $O: R \times R \rightarrow R$ \circ operație

- 1) $(R, +)$ grup comutativ
- 2) (R, \cdot) monoid
- 3) $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$
 $(a+b) \cdot c = a \cdot c + b \cdot c$

0 - elem neutru pt $+$
 1 - elem neutru pt \cdot

Reguli de calcul în inel

$$0 \cdot n = n \cdot 0 = 0$$

$$0 \cdot n = (0+0) \cdot n = 0 \cdot n + 0 \cdot n$$

$\exists n_1 \in R$ așa că $n_1 + 0 \cdot n = 0$

$$n_1 + 0 \cdot n + 0 \cdot n = 0 \Rightarrow 0 \cdot n = 0$$

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2$$

$\stackrel{3}{=} (a+b) \cdot a + (a+b) \cdot b$

Def $(R, +, \cdot)$ s.n. comutativ deci $a \cdot b = b \cdot a \quad \forall a, b \in R$

$$\begin{array}{l} (\mathbb{Q}, +, \cdot) ; (R, +, \cdot) \\ (\mathbb{Z}, +, \cdot) ; (\mathbb{C}^*, +, \cdot) \end{array}$$

Def. $(K, +, \cdot)$ se numește coprime cu $(K, +, \cdot)$ este
 inel $\Leftrightarrow \forall x \in K, x \neq 0 \Rightarrow \exists y \in K$ astfel încât $x \cdot y = y \cdot x = 1$
 Ex $(\mathbb{Z}_p, +, \cdot)$ coprime cu prim
 Ex \mathbb{C} de mai sus

Cuplul numerelor complexe

$$e^{ix} = \cos x + i \sin x$$

$$C = \{(a, b) \mid a, b \in R\}$$

$$(a, b) + (c, d) = (a+c, b+d) \quad (c, d) \cdot (e, f) = (ce+fd, cf+be)$$

$$a, b, c, d \in R$$

$$a+ib = c+id \Leftrightarrow \begin{cases} a=c \\ b=d \end{cases}$$

$$(a+ib) + (c+id) = a+c+i(b+d)$$

$$(a+ib)(c+id) = ac+bd+i(ed+bc)$$

$$re^{i\theta} = r(\cos \theta + i \sin \theta)$$

$$\begin{aligned} r &= \sqrt{a^2 + b^2} \\ \theta &= \tan^{-1} \frac{b}{a} \end{aligned}$$

$$z_1 = r_1 (\cos \theta_1 + i \sin \theta_1)$$

$$z_2 = r_2 (\cos \theta_2 + i \sin \theta_2)$$

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

Rundes kommutativ

$$\text{geht so: } (a+b)^n = C_0^n a^n + C_1^n a^{n-1} b + \dots + C_n^n b^n$$

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$$

$$\begin{aligned} \cos n\theta &= \cos \theta - C_2^n (\sin \theta)^2 + C_4^n (\cos \theta)^2 - \dots \\ \sin n\theta &= 1 - \cos^2 \theta \end{aligned}$$

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

$$f(x) = f'(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!}$$

$$g(x) = f(x) = c e^x \quad f(x) = c e^x$$

$$g'(x) = 0, g'(x) = \frac{f'(x) \cdot e^x - f(x) \cdot e^x}{e^{2x}} = \frac{f'(x) - f(x)}{e^x} = 0$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \dots$$

$$\sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!}$$

$$e^{ix} = 1 + \frac{ix}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} = \cos x + i \sin x$$

$$h(x) = f(x) + ig(x)$$
$$h'(x) = f'(x) + i g'(x)$$
$$= -g(x) + if(x) = h(x)$$

$$r(x) = \frac{h(x)}{e^{ix}} = r$$

$$r'(x) = \frac{h'(x)e^{ix} - h(x)e^{ix} \cdot i}{e^{2ix}} = 0$$

Algebra Cursul 2

 $(\mathbb{C}, +, \cdot)$ \leftarrow prelărime din cursul trecut. Momentan menționat.

$e^{ix} = \cos x + i \sin x$

$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots$ facut

$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \dots = f(x)$

$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \dots = g(x)$

$f'(x) = g(x)$

$g'(x) = f(x)$

Considera: $h(x) = \frac{f(x)}{\cos(x)}$ $h'(x) = \frac{f'(\cos x) - f(-\sin x)}{(\cos x)^2} = \frac{-g(x) \cos x + f(x) \sin x}{(\cos x)^2}$

$h''(x) = \frac{[-g'(x) \cos x + g(x) \sin x] \cos x - g(x) \sin x + f(x) \cos x}{\cos^4 x} = \frac{(-g(x) \cos x + f(x) \sin x) \cos x + (g(x) \cos x - f(x) \sin x)}{2 \cos^2 x}$

$h''(x) = \frac{2 \sin x}{(\cos x)^3} \cdot (-g(x) \cos x + f(x) \sin x)$

$h''(x) = h'(x) \cdot 2 \operatorname{tg} x$.

$f(x) = \sum_{m=0}^{\infty} \frac{f^{(m)}(0)}{m!} \cdot x^m$

$\cos^{(m)} x = \begin{cases} \cos x, & m=4k \\ -\sin x, & m=4k+1 \\ -\cos x, & m=4k+2 \\ \sin x, & m=4k+3 \end{cases}$

$\sin^{(m)} x = \begin{cases} \sin x, & m=4k \\ \cos x, & m=4k+1 \\ -\sin x, & m=4k+2 \\ -\cos x, & m=4k+3 \end{cases}$

$f(x) = \cos x : \cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \dots$

$f(x) = \sin x : \sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \dots$

$e^{ix} = 1 + \frac{ix}{1!} - \frac{x^2}{2!} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} - \frac{x^6}{6!} \dots$

$e^{ix} = \cos x + i \sin x$

Definiție

I $(R, +, \cdot)$ inel NOTAȚIE: $\cup(R) = \{n \in R \mid \exists s \in R \text{ astfel încât } n \cdot s = s \cdot n = 1\}$
 Lărgirea inversabilă ale inelului.

Ex: 1) $\cup(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ 2) $\cup(\mathbb{Z}[\sqrt{2}]) = \{\pm (1+\sqrt{2})^m \mid m \in \mathbb{Z}\}$ unde $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. R este corp $\Rightarrow \cup(R) = R \setminus \{0\}$

II Dacă $(R, +, \cdot)$ inel. S se numește subinel dacă
 $S \subseteq R$, $(S, +)$ grup $\begin{cases} \forall x \in S \quad x \in S \\ \forall x \in S \quad -x \in S \end{cases}$

III $(R, +, \cdot)$ inelI $\subset R$, I se numește ideal dacă

ideal $\begin{cases} \text{stang (a)} \\ \text{drept (b)} \\ \text{bilateral (c)} \end{cases}$

1) $\forall x, y \in I \Rightarrow x \cdot y \in I$ 2) a) $\forall r \in R, \forall i \in I \Rightarrow r \cdot i \in I$ b) $\forall r \in R, \forall i \in I \Rightarrow i \cdot r \in I$ c) $\forall r \in R, \forall i \in I \Rightarrow \left\{ \begin{array}{l} r \cdot i \in I \\ i \cdot r \in I \end{array} \right. \text{ și se numește } I \Delta R$

Obs: Dacă R este comutativ, mulțimile de ideal stang, drept, bilateral coincid.

Ex: $m\mathbb{Z} \triangleq \mathbb{Z} \quad \forall m \in \mathbb{N}^*$ $\forall I \Delta R \Rightarrow I = m\mathbb{Z}$ pt. un $m \in \mathbb{N}^*$ Mulțimea de polinoame cu coeficienți între-un inel comutativ R ($R[X]$) $f = (f_0, f_1, f_2, \dots, f_m, \dots) \quad f_j \in R \quad \forall j \in \mathbb{N} \quad \forall m \geq 0 \quad f_m = 0 \quad \forall m > m_0$ $R[X] \ni g = (g_0, g_1, \dots)$ $R[X] \ni f+g = (f_0+g_0, f_1+g_1, \dots, f_m+g_m, \dots)$ $f \cdot g = (f_0 \cdot g_0, f_0 \cdot g_1 + f_1 \cdot g_0, \dots, \sum_{j=0}^m f_j \cdot g_{m-j})$ Asociem $(0, 0, \dots, 0, 1, 0, \dots, 0) \xrightarrow[\text{not.}]{} x^m$ $f \in R[X]$ $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m \quad a_j \in R \quad a_m = \overline{a_m}$ ATENȚIE: Polinomul f nu este același lucru ca funcția polinomială asociată.Ex: $R = \mathbb{Z}_6 \quad f(x) = x^3 - x$ $f(\bar{0}) = \bar{0} \quad f(\bar{1}) = \bar{0} \quad f(\bar{2}) = \bar{0} \quad f(\bar{3}) = \bar{0} \quad f(\bar{4}) = \bar{0} \quad f(\bar{5}) = \bar{0}$

$f \in R[x]$

$$\text{grad } f = \begin{cases} m, & \text{dacă } a_m \neq 0 \\ -\infty, & \text{dacă } f = 0 \end{cases}$$

Ipoză: m rădăcini $\leq \text{grad } f$. nu este adevărat în totdeauna
 $\nexists f$

Def. $f \in R[x]$ $x_0 \in R$ s.m. rădăcina a polinomului f dacă $f(x_0) = 0$.

Proprietate: K corp.

$$x, y \in K, x \cdot y = 0 \Rightarrow x = 0 \text{ sau } y = 0$$

Dem. Presupun că $x \neq 0 \xrightarrow{K \text{ corp}} \exists z \in K \text{ a.t. } z \cdot x = 1$

$$x \cdot y = 0$$

$$z \cdot (x \cdot y) = z \cdot 0 = 0$$

$$\begin{array}{l} \parallel \quad \text{Riguri de calcul imed} \\ (z \cdot x) \cdot y = 1 \cdot y = y \end{array}$$

Inelul de polinoame cu coeficienți într-un corp comutativ K

Teorema împărțirii cu rest:

$f, g \in K[X], g \neq 0 \Rightarrow \exists q, r \in K[X]$ a.t. $f(x) = g(x) \cdot q(x) + r(x)$
 și $\text{grad } r < \text{grad } g$.

Demonstratie: Inductie după gradul lui f .

$$\begin{array}{ll} f=0 \text{ aleg } g=r=0 & \text{grad } 0 < \text{grad } g \in \mathbb{N} \\ 0=0 \cdot g(x)+0 & \end{array}$$

$f \neq 0$ Dacă $\text{grad } f < \text{grad } g$ aleg $g=0$ $r=f$.

Presupun eronul adevărat pentru $\text{grad } f = \{-m, 0, 1, \dots, \text{grad } g - 1, \dots, m\}$
 unde $m \geq \text{grad } g - 1$. Vreau să demonstreze eronul pentru $m+1$.

$$f(x) = a_{m+1}x^{m+1} + \dots + a_1x + a_0 \quad a_{m+1} \neq 0 \quad b_m \neq 0$$

$$g(x) = b_m x^m + \dots + b_1 x + b_0, \quad m+1 \geq m$$

Consider polinomul $h(x) = f(x) - g(x) \cdot x^{m+1-m} \cdot \frac{a_{m+1}}{b_m}$

Aplic ipoteza de inducție pentru h .

$$h(x) = -g(x) \cdot q_1(x) + r_1(x)$$

$$f(x) = \left[q_1(x) + x^{m+1-m} \cdot \frac{a_{m+1}}{b_m} \right] \cdot g(x) + r_1(x)$$

$$q_1(x) = q_1(x) + X$$

Afg C2
pag 4

$$\frac{x^{11}-1}{x-1} = x^{10} + x^9 + \dots + x + 1 = (x^2+2) \cdot g(x) + ax+b$$

$$x = i\sqrt{2} \quad (i\sqrt{2})^2 = -2$$

$$ai\sqrt{2} + b =$$

$$(i\sqrt{2})^{2k} = (-1)^k \cdot 2^k = (-2)^k$$

$$ai\sqrt{2} + b = ci\sqrt{2} + di \Rightarrow \begin{cases} a=c \\ b=d \end{cases}$$

$$a(i\sqrt{2} + b) = \frac{(i\sqrt{2})^{11}-1}{i\sqrt{2}-1} = \frac{-i\sqrt{2} \cdot 2^5 - 1}{i\sqrt{2}-1} = \frac{(i\sqrt{2} \cdot 32 - 1)(-1 - i\sqrt{2})}{3} = \frac{1 - 64 + i\sqrt{2}(1 + 32)}{3}.$$

$$= -21 + 11i\sqrt{2} = ai\sqrt{2} + b \Rightarrow a = 11, b = -21$$

Consecință: $g(x) = x - a$ este $f \in K[x]$

K corp comutativ $f(x) = g(x)(x-a) + b$ ~~acest~~ $b \in K$.

Prep $a \in K$ este rădăcină pentru ($\Rightarrow f(x) = g(x) \cdot (x-a)$) $g \in K[x]$

Tezumă K corp comutativ $\left\{ \begin{array}{l} f \in K[x] \text{ grad } f = m \geq 1 \\ g \in K[x] \text{ grad } g = n \end{array} \right\} \Rightarrow m$ rădăcini ale lui f este \leq grad $f = m$

Bem: Inductie după m.

$m=1$ $f(x) = ax + b$. f are doar o rădăcină $x = -\frac{b}{a}$ \textcircled{A}

Prusupun amintul adăverat pt m și demonstruz pt $m+1$

$f \in K[x]$ Cazul 1 $\text{grad } f = m+1$ Dacă f nu are rădăcini $\Rightarrow m$ răd $= 0 < m+1 = \text{grad } f \rightarrow 0$

Cazul 2: cînd f are rădăcină pentru f .

Folosesc proprietatea de mai sus $\Rightarrow f(x) = (x-a) \cdot g(x)$ $\text{grad } g = m$.

Fie b rădăcină pt $f \Rightarrow f(b) = 0 = (ba) \cdot g(b) \Rightarrow b-a=0$ sau $g(b)=0$
 $\Rightarrow \{ \text{rădăcini} \text{ lui } f \} = \{ a \} \cup \{ \text{rădăcini } g \}$

Aplic ipoteza de inducție $\Rightarrow m$ rădăcini $g \leq m \Rightarrow m$ răd $f \leq m+1$

Obo: K corp comutativ $\Rightarrow \text{grad } f \cdot g = \text{grad } f + \text{grad } g$.

Exemplu de corp necomutativ:

$$H = \{ a+bi+cj+dk \mid a, b, c, d \in R \}$$

$$i^2 = j^2 = k^2 = -1 \quad ij = k \quad ji = -k \quad ki = j \quad kj = -i \quad ik = j$$

$$a+bi+cj+dk = a_1+b_1i+c_1j+d_1k, \quad a, b, c, d, a_1, b_1, c_1, d_1 \in R \quad (\Rightarrow$$

$$x^2 = -1 \text{ ne răd } 3 \text{ rădăcini. Există } \infty \text{ infinitate.}$$

$$\begin{aligned} a &= a_1 \\ b &= b_1 \\ c &= c_1 \\ d &= d_1 \end{aligned}$$

CURS 3

TEOREMA: $f \in K[x]$, $\text{grad } f \geq 1$, K corp com.

Atunci:

$$\boxed{\text{nr. rădăcini } f \leq \text{grad } f}$$

CONSECINTĂ:

$$\begin{cases} p \text{ prim} & (\exists) \alpha \in \{1, 2, \dots, p-1\} \text{ a.i.} \\ (\mathbb{Z}_p^*, \cdot) \text{ ciclic} & \text{ord } \bar{\alpha} = p-1 \text{ în} \\ & (\mathbb{Z}_p^*, \cdot) \end{cases}$$

$$(G, \cdot) \leq (K^*, \cdot)$$

K corp comutativ $\Rightarrow G$ ciclic $(\exists) g \in G$ a.i.

G finit

$$G = \{g^k \mid k \in \mathbb{N}\}$$

Dacă aleg $K = \mathbb{Z}_p$ (p prim) $\Rightarrow (\mathbb{Z}_p^*, \cdot)$ ciclic

$$p=13 \quad (\mathbb{Z}_{13}^*, \cdot)$$

$$\mathbb{Z}_{13}^* = \{\bar{z}^k \mid k \in \mathbb{N}\}$$

$$\bar{2}^1 = 2 \quad \bar{2}^5 = \bar{6}$$

$$\bar{2}^2 = 4 \quad \bar{2}^6 = \bar{12}$$

$$\bar{2}^3 = \bar{8} \quad \bar{2}^7 = \bar{11}$$

$$\bar{2}^4 = \bar{3} \quad \bar{2}^8 =$$

$$\bar{2}^9 = \bar{5}$$

$$\bar{2}^{10} = \bar{10}$$

$$\bar{2}^{11} =$$

$$\bar{2}^{12} =$$

CRİPTARE CU CHEIE PUBLICĂ:

$$r \in \{1, \dots, p-1\}$$

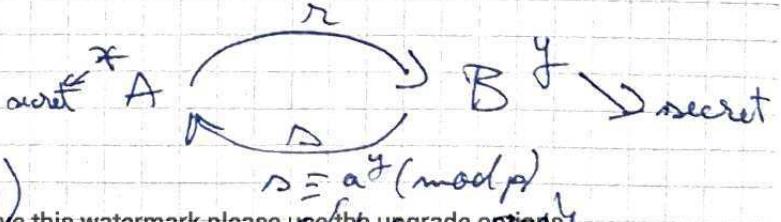
p prim mare public $r \equiv \alpha^x \pmod{p}$

α public

$$\alpha \in \{1, 2, \dots, p-1\}$$

$$\text{ord } \bar{\alpha} = p-1$$

$$\text{in } (\mathbb{Z}_p^*, \cdot)$$



$$A: \underset{P}{\overset{x}{\equiv}} (a^y)^x = a^{xy}$$

$$B: \underset{P}{\overset{y}{\equiv}} (a^x)^y = a^{xy}$$

IDEE DE DEMONSTRATIE:

$$m = \max \{\text{ord } g \mid g \in G\}$$

Voi arăta că $\boxed{\text{ord } g \mid m, \forall g \in G}$

presupun ord $v.$

$$|G| = n$$

$$\begin{matrix} m = \text{ord } h \\ h \in G \end{matrix} \Rightarrow m \mid n \Rightarrow m \leq n$$

$$(G, \cdot) \leq (K^*, \cdot) \quad f(x) = x^m - 1 \in K[x]$$

$$\downarrow \quad g \in G \Rightarrow \text{ord } g \mid m$$

$$\begin{matrix} \text{el. neutr.} \\ \text{al aceluiajui} \\ \text{grup.} \end{matrix} \quad g^m = (g^{\text{ord } g})^{\frac{m}{\text{ord } g}} = 1^{\frac{m}{\text{ord } g}} = 1 \Rightarrow f(g) = 0 \Rightarrow$$

$\Rightarrow g$ răd. pt. f

$$\boxed{\text{grad } f \geq \text{nr. răd. } f \geq |G| = n}$$

T. curs. precedent

$$\Rightarrow m = n$$

$$\text{ord } h = n$$

$$\left(1, h, h^2, h^3 \right) \subset G$$



$$|\{1, h, h^2, \dots\}| = n = |G|$$

PROP: (G, \cdot) grup. comutativ are

$$m = \max \{\text{ord } g \mid g \in G\}$$

Voi arata ca $\text{ord } g \mid m$

$\forall g \in G$

Remember: 1) $\text{ord } g \leq \frac{\text{ord } g}{(\text{ord } g, 1)}$

2) G e comutativ $(\text{ord } g_1, \text{ord } g_2) = 1$

$$\Rightarrow \text{ord } g_1 \cdot g_2 = \text{ord } g_1 \cdot \text{ord } g_2$$

$$m = \text{ord } h = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

p_i prim, $(\forall i=1, r)$

$$m = \text{ord } g = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$$

$p_i \neq p_j$ pt. $i \neq j$

$a_i, b_j \in \mathbb{N}$

Treb. sa arata ca $a_i \geq b_i$, $(\forall i=1, r)$

Arata ca $a_1 \geq b_1$

$$14 = 2^1 \cdot 5^0 \cdot 7^1$$

$$20 = 2^2 \cdot 5^1 \cdot 7^0$$

Pp. ca $a_1 < b_1$

$$\text{ord } g \cdot p_2^{b_2} \cdots p_r^{b_r} = \frac{\text{ord } g}{(\text{ord } g, p_2^{b_2} \cdots p_r^{b_r})} = p_1^{b_1}$$

$$\text{ord } g = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$$

$$\text{ord } h = \frac{p_1^{a_1}}{(\text{ord } h, p_1^{a_1})} = \frac{\text{ord } h}{p_1^{a_1}} = p_2^{a_2} \cdots p_n^{a_n}$$

$$\left(\text{ord} \left(g^{p_2^{b_2} \cdots p_n^{b_n}} \right), \text{ord } h^{p_1^{a_1}} \right) = 1$$

$$\stackrel{2)}{\Rightarrow} \text{ord} \left(g^{p_2^{b_2} \cdots p_n^{b_n}} \cdot h^{p_1^{a_1}} \right) = p_1^{b_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{if } m$$

Asta contrazice
maximul lui m.

Q.E.D.

$$p = 23$$

$$\mathbb{Z}_{23}^* = \{ \bar{1}, \bar{g}, \bar{g}^2, \dots \}$$

$$g \in \{1, 2, \dots, 22\} \quad \text{ord } \bar{g} = 22$$

$$2^{11} = 2048 \equiv 1 \pmod{23} \quad \text{ord } \bar{2} = 11$$

$$\text{ord } \bar{2}^2 = 2$$

$$(\text{ord } \bar{2}, \text{ord } \bar{2}^2) = (11, 2) = 1$$

$$\Rightarrow \text{ord } \bar{2} \cdot \bar{2}^2 = 2 \cdot 11 = 22$$

$$(12, 22) = 1$$

$$k \in \{0, 1, \dots, 21\}$$

$$k \in \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$$

$$\text{probabilitate} = \frac{10}{22} = \frac{5}{11}$$

TEOREMA WILSON: p -prim $\Rightarrow p \mid (p-1)! + 1$

Altă dem:

(care folosește polinoame) $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$

Sapt. prec: $f \in K[x]$

K corp comutativ

$\text{grad } f \geq 1$

$x_0 \in K$

x_0 radacina pt. $f \Leftrightarrow f(x) = g(x) \cdot h(x)$

$$\left. \begin{array}{l} p \text{ prim} \\ a \in \mathbb{Z} \\ p \nmid a \end{array} \right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

(Mici TEOREMA + LUI FERMAT)

$$f(\bar{1}) = 0 \quad f(\bar{j}) = 0, \quad (\forall) j \in \{1, 2, \dots, p-1\}$$

$$x^{p-1} - 1 = f(x) = (x - \bar{1})(x - \bar{2}) \dots (x - \bar{(p-1)})$$

$\bar{1}, \bar{2}, \dots, \bar{p-1}$ radacini lui f

$$\text{grad } f = p-1$$

$$g = \overline{2^1}$$

coefficientul în x^0 este $-\bar{1} = \overline{(p-1)!} \cdot \overline{(-1)^{p-1}}$

$$p \mid (p-1)! + 1$$

$$\left. \begin{array}{l} \text{Dacă } p > 2, \forall i \in \mathbb{Z}_{1,2} \\ (-1)^{2-1} = -\bar{1} = \bar{1} \end{array} \right\}$$



$$p | (p-1)! \left(\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1} \right)$$

Prop: p prim, $p \geq 5$

$$\Rightarrow p | (p-1)! \sum_{1 \leq i < j \leq p-1} i \cdot j$$

$$1 \leq i < j \leq p-1$$

FORMULELE LUI VIETE

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$$

$x_1, x_2, \dots, x_n \in K$ sunt rădăcinile f

[contolul cu multiplicitate] [

$$x \cdot f(x) = (x - x_1)^a \cdot g(x)$$

$$g(x_1) \neq 0$$

P.e. x_1 îl scriu de a ori

$$x_1 + x_2 + \dots + x_n =$$

coefficientul lui x^{n-1} : este $a_{n-1} = a_n(-x_1 - x_2 - \dots - x_n)$

$$x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n = \frac{a_{n-2}}{a_n}$$

$$x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_{n-2} x_{n-1} x_n = \frac{-a_{n-3}}{a_n}$$

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k} = \frac{(-1)^k a_{n-k}}{a_n}$$

\Rightarrow Există un corp comunitativ L , $K \subseteq L$ a.i.
 f are exact în rădăcini în L

$$2x+1=0 \quad \begin{matrix} z_1, z_2 \\ \in \mathbb{Q} \end{matrix}$$
$$z_1 \notin \mathbb{Q}$$
$$x^2+1=0 \quad \mathbb{R}$$

$$(x-i)(x+i)=0 \quad \mathbb{C}$$

$$a_n x^n + \dots + a_1 x + a_0 = 0 \quad a_j \in \mathbb{C}$$
$$(H) j=0, n$$

$$\Rightarrow \exists x_1, x_2, \dots, x_n \in \mathbb{C} \quad a_n \neq 0$$

rădăcini ale ec.

$$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$$

$$\{a+bi+cj+dk \mid a, b, c, d \in \mathbb{R}\}$$

$$i^2 = j^2 = k^2 = -1$$

$$i \cdot j = k; \quad j \cdot k = i; \quad k \cdot i = j$$

$$j \cdot i = -k; \quad k \cdot j = -i; \quad i \cdot k = -j$$

\mathbb{R} este inel comunitativ

$I \trianglelefteq \mathbb{R}$, I este ideal

dacă: 1) $(I, +)$ grup

2) $(H) r \in \mathbb{R}, (H) i \in I$

$\Rightarrow r \cdot i \in I$



Prop: $I \subseteq K[x]$

$$\Rightarrow \forall f \in K[x] \text{ a. n. } I - K[x] = \\ = \{f-g \mid g \in I\}$$

Dem: Dacă $I = \{0\}$ aleg $f = 0$

Dacă $\{0\} \subseteq I$ aleg $f \in I$, $f \neq 0$

a. i. $\text{grad } f = \underline{\text{rest}}$

$$= \min \{ \text{grad } g \mid g \in I \setminus \{0\} \}$$

$$f(K[x]) = I \\ \leq^* \text{"banal"}$$

$$\geq^* \text{Aleg } h \in I \xrightarrow[\text{in rest}]{\substack{T-\text{imp.}}} h = f - g + r$$

$$g, r \in K[x]$$

$$\text{grad } r < \text{grad } f$$

$$r = h - f \in I$$

$$f \in I, g \in K[x] \Rightarrow f - g \in I$$

$$\text{zD, } r = 0$$

conform alegerei lui f



$$1 \cdot \dots \cdot m = p_1 \cdot \dots \cdot p_t$$

15.03.2018

Algebra
- curs 4 -

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

Prop. $I \subseteq K[x] \Rightarrow I = f \cdot K[x] = \{f \cdot g \mid g \in K[x]\}$
 $\exists f \in K[x]$ a.t.

Analogia $K[x] \rightarrow \mathbb{Z}$

Th. împ cu rest. numere întregi

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

Th. împ. cu rest polinoame

$f, g \in K[x], g \neq 0 \Rightarrow \exists q, r \in K[x]$ a.t. $f = g \cdot q + r,$
 $\text{grad } r < \text{grad } g$

În \mathbb{Z} : $\forall m \in \mathbb{Z}, m \neq 0$ se scrie $m = \pm p_1^{a_1} \cdots p_n^{a_n}, p_i - \text{prim}$
 $m \neq \pm 1$

$\frac{+}{\times} \frac{j}{i} = \frac{1}{r}$
Scrisa e unică, dar ordinea factorilor nu.

Teorema fundamentală a aritmeticii

Def $f \in K[x]$, grad $f \geq 1$ se numește ireductibil dacă nu se poate scrie $f = g'h$, unde $g, h \in K[x]$ și grad $g < \text{grad } f$, grad $h \leq \text{grad } f$.
 polinomul ireductibil \rightarrow nr prim din

Analogul teoremei fundamentale a aritmeticii pe K :

$\forall f \in K[x], f \neq 0$, grad $f \geq 1$ se scrie, unică, ca produs de polinoame ireductibile.

Că înțeleg prin "unic"? $f = f_1 f_2 \dots f_m$, $f_i \in K[x]$ ireductibili.

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

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

Dem obs. 2. $\exists k \in K^*$ $k \cdot k^{-1} = 1$

\subseteq Fie $f \in U(K[x]) \Rightarrow \exists g \in K[x]$ a.i.
 $f \cdot g = 1 \Rightarrow \text{grad } f + \text{grad } g = 0 \Rightarrow$
 $\text{grad } g = \text{grad } f = 0, f \in K^*$

Contraexemplu: $Z_{100}[x] \quad (3 + \sqrt{10}x)(\bar{a} + \bar{b}x) = 1$

$$\bar{3} \cdot \bar{a} = 1 \quad | \quad \bar{10} \cdot \bar{b} = 0, b = 10k, k \in Z$$

$$\begin{cases} 33 \cdot 3 = -1 \\ (-33) \cdot 3 = 1 \end{cases} \Rightarrow a = 67$$

$$3\bar{b} + \bar{10}\bar{a} = 0 \quad 30k + 670 = 0 \Rightarrow 30k = \bar{670}$$

$$\text{Aleg } k=1 \quad 100 \mid 30(k-1) \Rightarrow 10 \mid k-1$$

Adăos: $f \in K[x]$ | $\Rightarrow f$ se scrie unică
 $\text{grad } f \geq 1$

$$f = k \cdot f_1 \cdot f_2 \dots f_n, k \in N^*$$

f_j ireductibil și monic, $\nexists j = 1, n$

$\exists x \in (\mathbb{R}, +, \cdot)$ astfel că $x \in U(\mathbb{R})$

\Rightarrow există un număr de inversare ca

$\exists m \in \mathbb{N}^*$ a.s. $x^m = 0$. Arătăm că $x + x \in U(\mathbb{R})$

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

$$(-x)^m = 0 \quad (\text{din faptul că } x^m = 0)$$

$$x^{m+1} - (-x)^m = (x+x)(\dots + \dots + \dots)$$

$\Rightarrow x+x$ inversabil

singuratic-marek

$f \in K[X]$ se numește monic dacă

$$f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$$

O altă analogie CMMDC

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

$d \in \mathbb{N}^*$ s.t.

$\begin{cases} d \mid a \\ d \mid b \end{cases}$

$\forall e \in \mathbb{Z}, e \mid a \wedge e \mid b \Rightarrow e \mid d$.

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

$h = (f, g) = \text{c.m.m.d. } c$ al polinoamelor f, g

$\in K[X]$ monic

$\begin{cases} h \mid f \\ h \mid g \end{cases}$

Dacă $h \mid g$ și $h \mid f \Rightarrow h \mid h$.

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

$$f = k_1 \cdot f_1^{a_1} \cdot f_2^{a_2} \cdots f_n^{a_n}, \text{ } f_i \text{-irreductibile monice}$$

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

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

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

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

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

$$(21, 36) = 3.$$

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

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

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

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

$\exists m, n \in \mathbb{Z}$ a.s. $a \cdot m + b \cdot n = (a, b)$

Dem bazată pe th. împărțiri cu rest.

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

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

Algoritmul RHO al lui Pollard nu se amintește

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

$f \in \mathbb{Z}[X]$, grad $f = 2$. Azi se foloseste $f(x) = x^2 - 1$

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

Algebra C5

Inel factor

$(R, +, \cdot)$ inel

Ideal bilateral al lui R ($J \trianglelefteq R$)

1) $(J, +)$ grup

2) $\forall r \in R, \forall i \in J \Rightarrow \begin{cases} i \cdot r \in J \\ r \cdot i \in J \end{cases}$

Analogie cu constructia grupului factor

$$\frac{R}{J} \quad \overline{n_1} = \overline{n_2} \Leftrightarrow n_1 - n_2 \in J$$

$n_1, n_2 \in R$

$$\text{Definim } +, \cdot \quad \overline{n_1} + \overline{n_2} \stackrel{\text{def}}{=} \overline{n_1 + n_2}$$

$$\overline{n_1} \cdot \overline{n_2} \stackrel{\text{def}}{=} \overline{n_1 \cdot n_2}$$

Definitia este corecta

$(\frac{R}{J}, +)$ grup com

$(\frac{R}{J}, +)$ grup factor

$$\text{Trebue sa aratam ca: } \frac{\overline{n_1} = \overline{s_1}}{\overline{n_2} = \overline{s_2}} \quad \left| \begin{array}{l} ? \Rightarrow \overline{n_1} \cdot \overline{n_2} = \overline{s_1} \cdot \overline{s_2} \\ \frac{||}{\overline{n_1 \cdot n_2}} \stackrel{?}{=} \frac{||}{\overline{s_1 s_2}} \end{array} \right.$$

$n_1, n_2, s_1, s_2 \in R$

Trebue sa arat ca $n_1 \cdot n_2 - s_1 \cdot s_2 \in J$

$$\overline{n_1} = \overline{s_1} \Rightarrow n_1 = s_1 + i_1$$

$$n_2 = s_2 + i_2$$

$$i_1, i_2 \in J$$

$$n_1 \cdot n_2 - s_1 \cdot s_2 = (s_1 + i_1)(s_2 + i_2) - s_1 \cdot s_2 = \underset{J}{\cancel{s_1 \cdot i_2}} + \underset{J}{\cancel{i_1 \cdot s_2}} + \underset{J}{\cancel{i_1 \cdot i_2}} \in J \quad (\text{pt ca } (J, +) \text{ este grup})$$

$\Rightarrow (\frac{R}{J}, +, \cdot)$ inel factor

Exemplu:

$$(\mathbb{Z}_n, +, \cdot)$$

Teorema fundamentală de izomorfism pentru inele

Def: $(R_1, +, \cdot)$, $(R_2, +, \cdot)$ inele. O funcție $f: R_1 \rightarrow R_2$ s.n. morfism de inele dacă:

- 1) $f(x+y) = f(x) + f(y) \quad \forall x, y \in R_1$
- 2) $f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R_1$
- 3) $f(1_1) = 1_2$

0_1 - elem. neutrul $(R_1, +)$

0_2 - e. n. pt. $(R_2, +)$

1_1 - elem. neutrul pt (R_1, \cdot)

1_2 - e. n. pt (R_2, \cdot)

$$\text{Ker } f = \{r \in R_1 \mid f(r) = 0_2\}$$

$$\text{Im } f = \{f(r) \mid r \in R_1\}$$

TFI pt. inele

$(R_1, +, \cdot)$, $(R_2, +, \cdot)$ inele

$f: R_1 \rightarrow R_2$ morfism de inele. Atunci

$$\frac{R_1}{\text{Ker } f} \cong \text{Im } f$$

$(S_1, +, \cdot)$, $(S_2, +, \cdot)$ inele

Spunem că inelele S_1 și S_2 sunt izomorfe ($S_1 \cong S_2$) dacă

$\exists g: S_1 \rightarrow S_2$ morfism de inele și g e fc. bijectivă

Dem analogica cu cea de la TFI grupuri

$\text{Ker } f \subseteq R_1$ (ideal bilateral)

$$r_1, r_2 \in \text{Ker } f \Rightarrow r_1 + r_2 \in \text{Ker } f$$

$$r_1 \cdot r_2 \in \text{Ker } f$$

$$a \in R_1 \xrightarrow{?} a \cdot r_1 \in \text{Ker } f$$

$$r_1 \cdot a \in \text{Ker } f$$

- e -

$$f(\lambda_1) = 0_2$$

$$f(\lambda_2) = 0_2$$

$$f(\lambda_1 + \lambda_2) = f(\lambda_1) + f(\lambda_2) = 0_2 + 0_2 = 0_2$$

$$f(\lambda_1 - \lambda_2) = f(\lambda_1) - f(\lambda_2) = 0_2 - 0_2 = 0_2$$

$$f(a \cdot \lambda_1) = f(a) \cdot f(\lambda_1) = f(a) \cdot 0_2 = 0_2$$

$$f(\lambda_1 \cdot a) = f(\lambda_1) \cdot f(a) = 0_2 \cdot f(a) = 0_2$$

Dem TFI inel

$$g : \frac{R_1}{Ker f} \rightarrow Im f$$

$$g(\bar{\lambda}_1) \stackrel{\text{def}}{=} f(\lambda_1)$$

g bine definită

$$\bar{\lambda}_1 = \bar{\lambda}_2 \stackrel{?}{\Rightarrow} g(\bar{\lambda}_1) = g(\bar{\lambda}_2)$$

$$\lambda_1 = \lambda_2 + i$$

$$i \in Ker f \quad f(i) = 0_2$$

$$g(\bar{\lambda}_1) \stackrel{\text{def}}{=} f(\lambda_1) = f(\lambda_2 + i) = f(\lambda_2) + f(i) = f(\lambda_2) + 0_2 = f(\lambda_2) = g(\bar{\lambda}_2)$$

f mon. de inele

Pasii:

$$1) g(\bar{\lambda}_1 + \bar{\lambda}_2) = g(\bar{\lambda}_1) + g(\bar{\lambda}_2) \quad \forall \lambda_1, \lambda_2 \in R_1$$

$$2) g(\bar{\lambda}_1 \cdot \bar{\lambda}_2) = g(\bar{\lambda}_1) \cdot g(\bar{\lambda}_2) \quad \forall \lambda_1, \lambda_2 \in R_1$$

$$3) g(\bar{\lambda}_1) = 1_2$$

4) g bij

$$1) g(\bar{\lambda}_1 + \bar{\lambda}_2) = g(\bar{\lambda}_1 + \bar{\lambda}_2) \stackrel{\text{def}}{=} f(\lambda_1 + \lambda_2) = f(\lambda_1) + f(\lambda_2) = g(\bar{\lambda}_1) + g(\bar{\lambda}_2)$$

$$3) g(\bar{\lambda}_1) = f(1_1) = 1_2$$

4) - surjectivitatea e evidentă

- injectivitatea: $g(\bar{\lambda}_1) = g(\bar{\lambda}_2) \stackrel{?}{\Rightarrow} \bar{\lambda}_1 = \bar{\lambda}_2$

$$f(\lambda_1) = f(\lambda_2)$$

$$f(n_1 - n_2) = f(n_1) - f(n_2) = 0_2$$

$$\Rightarrow n_1 - n_2 \in \text{Ker } f \Rightarrow \overline{n_1 - n_2} = \overline{0} \Rightarrow \overline{n_1} = \overline{n_2}$$

2. Altă teorema de izomorfism

$(R, +, \cdot)$ inel com.

$$J \subseteq J \subseteq R$$

$$\Rightarrow \frac{R}{J} \cong \frac{R}{J}$$

$$\frac{J}{J} \trianglelefteq \frac{R}{J}$$

Ex: $(R, +, \cdot)$ inel

$$J \trianglelefteq R$$

În ce situație se poate întâmpla ca $1 \in J$?

$$(v \in J)$$

$$v \in U(R)$$

Obs: K, L corpuri, $f: K \rightarrow L$ morfism de corpuri $\Rightarrow f$ inj.

Dem: fie $x, y \in K$ a.t. $f(x) = f(y)$. Trebuie să arăt că $x = y$.

Presupun că $x \neq y \Rightarrow x - y \neq 0_K \Rightarrow \exists z \in K$ a.t. $(x - y) \cdot z = z(x - y) = 1_K$

$$1_L = f(1_K) = f((x - y) \cdot z) = f(x - y) \cdot f(z) = (\underbrace{f(x) - f(y)}_{0_K}) \cdot f(z) = 0_L \cdot f(z) = 0_L$$

\Downarrow

$$\left(\begin{array}{l} f(x) - f(y) = f(x - y) \\ f(x - y) + f(y) = f((x - y) + y) = f(x) \end{array} \right)$$

$$K \cong f(K), \quad f(K) \subseteq L$$

$$K \leq L$$

Polinoame simetrice

R inel comutativ $R[X]$ - inelul de polinoame cu coef. in R

$$R[x_1, x_2, \dots, x_n]$$

Linel de polinoame cu coef.
in R , in nedeterminatele

$$x_1, x_2, \dots, x_n$$

$$R[x_1]$$

$$R[x_1, x_2] \stackrel{\text{def}}{=} R[x_1][x_2]$$

dacă considerăm
un inel S

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

Def: f. s.n. simetric dacă $f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, \dots, x_{\sigma(n)}) = f(x_1, x_2, \dots, x_n)$

$$f(x_1, x_2) = x_1^2 \cdot x_2^3 + x_1^3 \cdot x_2^2 + x_1^2 \cdot x_2^3 \quad \forall \sigma \in S_2 \quad \text{e simetric? Nu}$$

$$(S_n = \{ \sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \})$$

$$f(x_1, x_2) = x_1^2 \cdot x_2^3 + x_1^3 \cdot x_2^2 + x_1^2 \cdot x_2^2 + x_1 \cdot x_2^2 \quad \text{e simetric}$$

$$f(x_2, x_1) = x_2^2 \cdot x_1^3 + x_2^3 \cdot x_1^2 + x_2^2 \cdot x_1 + x_2 \cdot x_1^2 = f(x_1, x_2) \quad \sigma \text{ bij}$$

$$f(x_1, x_2, x_3) = x_1^2 \cdot x_2 + x_1 \cdot x_2^2 + x_2 \cdot x_3^2 + x_2^2 \cdot x_3 + x_1 \cdot x_3^2 + x_3 \cdot x_1^2 = S_1 S_2 - 3 S_3$$

Exemplu de pol. sim.

$$\begin{cases} S_1(x_1, x_2, \dots, x_n) = x_1 + x_2 + x_3 + \dots + x_n \\ S_2(x_1, x_2, \dots, x_n) = x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + x_2 x_3 + x_2 x_4 + \dots + x_2 x_n + \dots + x_{n-1} x_n \\ S_3(x_1, \dots, x_n) = x_1 x_2 x_3 + x_1 x_2 x_4 + \dots \\ \vdots \\ S_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n \end{cases}$$

↑ polinoame simetrice fundamentale

$$\begin{aligned} f(x_1, x_2) &= x_1^2 \cdot x_2^3 + x_1^3 \cdot x_2^2 + x_1^2 \cdot x_2 + x_2^2 \cdot x_1 = x_1 x_2 [x_1 x_2^2 + x_1^2 x_2 + x_1 + x_2] = \\ &= S_2 [S_1 + S_1 S_2] = S_1 S_2 + S_1 S_2^2 \end{aligned}$$

Teorema fundamentală a polinoamelor simetrice

$$\begin{cases} f \in R[x_1, \dots, x_n] \\ f \text{ simetric} \end{cases} \Rightarrow \exists g \in R[x_1, \dots, x_n] \text{ a.t. } f(x_1, \dots, x_n) = g(S_1(x_1, \dots, x_n), S_2(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n))$$

Algorithm de calcul pt. g

$$S_1^2 - 2S_2$$

1) descompunerea în componentă omogenă

2) detectarea monoamelor $s_1^{a_1} s_2^{a_2} \dots s_n^{a_n}$ care apar

componentă omogenă de grad K (4) care nu este mai mult decât coeficientul maxim.

Trebuie să găsească „foate”

$$k_1 \geq k_2 \geq \dots \geq k_n \geq 0 \quad k_j \in \mathbb{N} \forall j$$

$$\sum_{j=1}^n k_j = K$$

$j=1$ le iau lexicografic, descreșcător
 Posibilități $(3, 1, 0)$ $3+1+0=4$

$\begin{pmatrix} 2, 2, 0 \\ 2, 1, 1 \end{pmatrix} \rightarrow$ au niste coeficienti

$$S_1^{K_1-K_2} \cdot S_2^{K_2-K_3} \cdot S_3^{K_3-K_4} \cdots S_{n-1}^{K_{n-1}-K_n} \cdot S_n^{K_n}$$

$$(3, 1, 0) \rightarrow S_1^{3-1} S_2^{1-0} S_3^0 = S_1^2 S_2$$

$$(2,2,0) \rightarrow S_1^{2-2} S_2^{2-0} S_3^0 = S_2^2$$

$$(2,1,1) \rightarrow S_1 S_2^0 S_3 = S_1 S_3$$

$$\text{Comp. omogena: } \cancel{x_1^3} + x_1^3 x_2 + x_1 x_2^3 + x_1^3 x_3 + x_1 x_3^3 + x_2^3 x_3 + x_2 x_3^3 = S_1^2 S_2 + A \cdot S_2^2 +$$

3) *Aflecta* *coef.* *monoamelor*

P.L. a det. coef A și B dăm valori nedeterminate;

$$\begin{array}{ll} x_1 = 1 & S_1 = 2 \\ x_2 = 1 & S_2 = 1 \\ x_3 = 0 & S_3 = 0 \end{array}$$

$$f(1, 1, 0) = 2 = 4 + A \Rightarrow \underline{A = -2}$$

$$\begin{array}{ll} X_1 = 1 & S_1 = 3 \\ X_2 = 1 & S_2 = 3 \\ X_3 = 1 & S_3 = 1 \end{array}$$

$$f(3, 1, 1) = 6 = 27 + (-2) \cdot 9 + 3 \cdot 3 = 9 + 3 \cdot 3$$

$$\Rightarrow 6 = 9 + 3B \Rightarrow 3B = -3 \Rightarrow B = -1$$

Algebra Curs B.

Teorema fundamentală a polinoamelor simetrice.

Def. polinom simetric.

R-imele comutativ. $f \in R[x_1, x_2, \dots, x_m]$ se numește polinom simetric dacă $f(x_1, x_2, \dots, x_m) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(m)}) \forall \sigma \in S_m$.TFP R-imele comutativ. $f \in R[x_1, \dots, x_m]$ nu este simetric.Atunci există $g \in R[x_1, \dots, x_m]$ a.i. $f(x_1, \dots, x_m) = g(\alpha_1, \alpha_2, \dots, \alpha_m)$

$$\alpha_1(x_1, x_2, \dots, x_m) = x_1 + x_2 + \dots + x_m$$

$$\alpha_2(x_1, x_2, \dots, x_m) = x_1 x_2 + x_1 x_3 + \dots + x_{m-1} x_m$$

$$\alpha_k(x_1, \dots, x_m) = x_1 x_2 \dots x_k + \dots \quad \text{grad } \alpha_k = k.$$

$$\alpha_m(x_1, \dots, x_m) = x_1 \cdot x_2 \cdot \dots \cdot x_m.$$

Algoritm pentru aflarea lui g . (R-imele comutativ)

$$\text{grad}(x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}) = a_1 + a_2 + \dots + a_m.$$

1) Descompunerea în componente "simogene" (monomii cu același grad).

Exemplu: $f(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^3 + x_1^3 x_2^3 + x_1^3 x_3^3 + x_2^3 x_3^3$

Luăm R-imele comutativ

2) Lăruim pe componente "simogene" de grad d.

Găsesc monomul $a \cdot x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$

$$k_1 + k_2 + \dots + k_m = d \quad k_1 \geq k_2 \geq \dots \geq k_m \geq 0.$$

Dacă găsesc 2 monomii cu același k_1 maxim, și le adug pe cel cu k_2 maxim.Găsesc toate soluțiile $\begin{cases} t_1 + t_2 + \dots + t_m = d \\ k_1 \geq t_1 \geq t_2 \geq \dots \geq t_m \geq 0 \end{cases} \quad t_j \in \mathbb{N} \quad k_i \in \mathbb{N} \quad \sum t_j = d \leq m$ O astfel de soluție produce monomul $\alpha_1^{t_1} \alpha_2^{t_2} \dots \alpha_m^{t_m} \cdot \alpha_{m+1}^{d-t_1-t_2-\dots-t_m}$.

$$1 \cdot (t_1 - t_2) + (t_2 - t_3) + 2 + 3(t_3 - t_4) + \dots + (t_{m-1} - t_m)(m-1) = \\ = t_1 + t_2 + t_3 + \dots + t_m = d$$

3) Găsirea coeficienților. (se dau valori lui x_1, \dots, x_m).

Continuăm pe exemplu:

$$g(x_1, x_2, x_3) = x_1^4 + x_2^4 + x_3^4 = \alpha_1^4 + A \cdot \alpha_1^2 \alpha_2 + B \alpha_2^2 + C \alpha_1 \alpha_3.$$

$$x_1^4 \cdot x_2^0 \cdot x_3^0 \rightarrow (4, 0, 0) \Rightarrow 4 \geq t_1 \geq t_2 \geq t_3 \geq 0 \quad t_1 + t_2 + t_3 = 4.$$

$$\begin{matrix} 3, & 1, & 0 \\ 2, & 2, & 0 \\ 1, & 1, & 1 \end{matrix}$$

$$(1, 0, 0) \rightarrow \alpha_1$$

$$(3, 1, 0) \rightarrow \alpha_1^2 \alpha_2$$

$$\begin{matrix} (2, 2, 0) \rightarrow \alpha_2^2 \\ (2, 1, 1) \rightarrow \alpha_1 \alpha_3 \end{matrix}$$

$$A = ?$$

$$B = ?$$

$$C = ?$$

HAGL6
 pagina .

$$\Delta_1 = x_1 + x_2 + x_3$$

$$\Delta_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$$

$$\Delta_3 = x_1 x_2 x_3$$

$$\begin{cases} x_1 = 1 & x_2 = 1 \\ x_3 = -\frac{1}{2} \end{cases} \Rightarrow \begin{aligned} \Delta_1 &= \frac{3}{2} & \Delta_3 &= -\frac{1}{2}, \\ \Delta_2 &= 0 \end{aligned}$$

$$g(1, 1, -\frac{1}{2}) = \frac{81}{16} + C \cdot \left(-\frac{3}{4}\right) = 2 + \frac{1}{16} \Rightarrow$$
$$\Rightarrow 33 = 81 - 12C \Rightarrow 12C = 48 \Rightarrow C = 4$$

$$\begin{cases} x_1 = x_2 = 1 \\ x_3 = 0 \end{cases} \Rightarrow \begin{aligned} \Delta_1 &= 2 \\ \Delta_2 &= 1 \\ \Delta_3 &= 0 \end{aligned}$$

$$g(1, 1, 0) = 16 + 4A + B = 2 \Rightarrow A + B = -14,$$

$$\begin{cases} x_1 = x_2 = x_3 = 1 \Rightarrow \\ \Delta_1 = 3 \\ \Delta_2 = 3 \\ \Delta_3 = 1 \end{cases}$$

$$g(1, 1, 1) = 81 + 27A + 9B + 12 = 3$$

$$27A + 9B = -90 \Rightarrow 3A + B = -10,$$
$$\begin{cases} 4A + B = -15 \\ 3A + B = -10 \end{cases} \Rightarrow \begin{aligned} 4A - 3A &= -15 - (-10) \\ A &= -5 \end{aligned}$$

$$A = -5 \quad B = 2 \quad C = 4$$

Exemplu 2: $f(x_1 x_2 x_3) = x_1^3 x_2^3 + x_1^3 x_3^3 + x_2^3 x_3^3 = \Delta_2^3 + A \Delta_1 \Delta_2 \Delta_3 + B \cdot \Delta_3^2$

$$\Delta_2^3 \leftarrow (3, 3, 0) \quad 3 \geq t_1 \geq t_2 \geq t_3 \geq 0$$

$$\Delta_1 \Delta_2 \Delta_3 \leftarrow (3, 2, 1)$$

$$\Delta_3^2 \leftarrow (2, 2, 2)$$

$$f(1, 1, -2) = 1 - 8 - 8 = -15 = -27 + 4B \Rightarrow 4B = 12 \Rightarrow B = 3 \rightarrow \begin{aligned} x_1 &= 1 & x_2 &= 1 & x_3 &= 2 \\ \Delta_1 &= 0 & \Delta_2 &= 0 & \Delta_3 &= -2 \end{aligned}$$

$$x_1 = x_2 = x_3 = 1 \quad \Delta_1 = 3 \quad \Delta_2 = 3 \quad \Delta_3 = 1$$

$$3 = f(1, 1, 1) = 27 + 9A + 3 \Rightarrow 9A = -27 \Rightarrow A = -3,$$

Teorema fundamentală a algebrui:

$f \in \mathbb{C}[x]$, $\underbrace{\text{grad } f \geq 1}_{m} \Rightarrow \exists z \in \mathbb{C} \text{ a r. } f(z) = 0$

Consecință $\exists z_1, z_2, \dots, z_m \in \mathbb{C}$ a.r. $f(x) = a(x - z_1)(x - z_2) \dots (x - z_m)$

Schită de demonstrație:

a) $f \in \mathbb{R}[x]$ și $\text{grad } f = \text{impar}$ $\Rightarrow f$ are o rădăcimă reală

$$f(x) = a x^{m+1} + b x^m + \dots + c = 0 \quad a \neq 0$$

$a > 0 \quad \lim_{x \rightarrow \infty} f(x) = \infty \quad \lim_{x \rightarrow -\infty} f(x) = -\infty \Rightarrow f(x_0) > 0 \quad f(x_1) < 0 \quad f \text{ cont.}$

$$\Rightarrow \exists x_2 \in (x_0, x_1) \text{ a.r. } f(x_2) = 0$$

b) $a z^2 + bz + c = 0 \quad a, b, c \in \mathbb{C}, \quad a \neq 0$
 rădăcinile ecuației sunt complexe $z_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a} \quad \Delta = b^2 - 4ac.$

$$z = r(\cos\theta + i\sin\theta)$$

$$\sqrt{z} = \sqrt{r} \left(\cos \frac{\theta}{2} + i \sin \frac{\theta}{2} \right) \cong \sqrt{r} \left(\cos \left(\frac{\theta}{2} + \pi \right) + i \sin \left(\frac{\theta}{2} + \pi \right) \right)$$

$$\cos \pi + i \sin \pi = -1. \quad e^{i\pi} = -1.$$

c) $f \in \mathbb{R}[x]$ grad $f \geq n \Rightarrow \exists z \in \mathbb{C}$ a.c. $f(z) = 0$.

$$\text{grad } f = 2^k \cdot m, \quad m \text{ impar}$$

Inductie după n .

Vezi că $\beta = 0$ (punctul a)

$n \in \mathbb{N}^*$, presupunem enuntul aduferat pentru $m \leq n-1$

Teorema K corp comutativ. $f \in K[x]$ grad $f = m \Rightarrow$

$\Rightarrow \exists L$ corp. com. a.i. $K \leq L$ a.t. f are m rădăcini în L .

Fie $L \geq \mathbb{R}$ a.u. $t_1, t_2, \dots, t_m \in L$ sunt rădăcinile lui f . L corp. com,

$$1 \leq j < j' \leq m, \quad a \in \mathbb{R} \text{ fixat.}$$

$$m_{ij}(a) = (t_i + t_j) \cdot a + t_i \cdot t_j.$$

$$\text{Construiesc } g(x) = \prod_{j=1}^m (x - m_{ij}(a))$$

$$\textcircled{*} \quad \text{grad } g = C_m = \frac{m(m-1)}{2} = 2^{n-1} \cdot \frac{(m-1)}{2} \quad \text{impar}$$

$$n \in \mathbb{N}^* \Rightarrow m \text{ par} \Rightarrow m-1 \text{ impar.}$$

(*) $g \in \mathbb{R}[x]$

Coefficienți lui g (văzută ca mediterată) polinoame
 în t_1, \dots, t_m , pol. simetrică. TPS coeficient $(t_1, \dots, t_m) = h(s_1, \dots, s_m)$
 $h \in \mathbb{R}[x_1, \dots, x_m]$

$$s_K(t_1, \dots, t_m) = t_1 t_2 \dots t_k + \dots = (-1)^K \frac{a_{m-k}}{a_m} \quad (\text{Viète}) \quad g \in \mathbb{R}[x]$$

Apl. ipoteza de inducție: pt. fiecare $a \in \mathbb{R}$

$\xrightarrow{\text{ip. ind.}} \forall 1 \leq i < j \leq m$ a.t. $m_{ij}(a) \in \mathbb{C}$

$$\exists C_m^2 \text{ perechi } (i, j) \quad 1 \leq i < j \leq m. \Rightarrow$$

$$\Rightarrow \exists a, b \in \mathbb{R} \quad a + b \text{ a.t. } m_{ij}(a) \in \mathbb{C} \quad \text{a.t. } m_{ij}(b) \in \mathbb{C}$$

$$\begin{cases} (t_i + t_j)a + t_i t_j \in \mathbb{C} \\ (t_i + t_j)b + t_i t_j \in \mathbb{C} \end{cases} \text{ le scad } \Rightarrow (b-a)(t_i + t_j) \in \mathbb{C}$$

$t_i, t_j \in L$ sunt rădăcinile ecuației $t_i, t_j \in \mathbb{C}$

$$x^2 - px + q = 0 \quad p, q \in \mathbb{C} \xrightarrow{b} t_i, t_j \in \mathbb{C}$$

Alg. C6
pag 4

d) $f \in \mathbb{C}[X]$, $\text{grad } f \geq 1 \Rightarrow \exists z \in \mathbb{C} \quad f(z)=0$.

$$g(x) = f(x) \cdot \bar{f}(x) \quad a_k \neq 0 \quad g(x) \in \mathbb{R}[x] \quad (*)$$
$$f(x) = a_k x^k + \dots + a_1 x + a_0 \in \mathbb{C}[x]$$

$$\bar{f}(x) = \bar{a}_k x^k + \dots + \bar{a}_1 x + \bar{a}_0$$

$$\dim (*) \Leftrightarrow \exists z \in \mathbb{C} \text{ a.r. } g(z) = 0 = f(z) \cdot \bar{f}(z) = 0 \Rightarrow \begin{cases} f(z) = 0 \\ \bar{f}(z) = 0 \end{cases} \text{ sau}$$

Dacă $\bar{f}(z) = 0$

$$\bar{a}_k \cdot \bar{z}^k + \bar{a}_{k-1} \bar{z}^{k-1} + \dots + \bar{a}_1 \bar{z} + \bar{a}_0 = 0$$

$$a_k z^k + a_{k-1} z^{k-1} + \dots + a_1 z + a_0 = 0.$$

d) $\exists z \in \mathbb{C}$ a.r. $f(z) = 0$

$$f(x) = a(x-z)f_1(x) \quad f_1 \in \mathbb{C}[X], \quad \text{grad } f_1 = m-1. \quad \text{Aplic ip. înd.}$$

Gauss: $x = ame$

a este restul împărțirii lui x la 19.

$$b \quad - \quad \overline{\overline{\quad}} \quad \text{la 4.}$$

$$c \quad - \quad \overline{\overline{\quad}} \quad \text{la 7.}$$

$$d \quad - \quad \overline{\overline{\quad}} \quad 19a+15 \quad \text{la 3d}$$

$$e \quad - \quad \overline{\overline{\quad}} \quad 2b+4c+6d+6 \quad \text{la 7.}$$

Paste: $= d+e+4$ aprileie dacă $d+e+4 \leq 30$

$$= [(d+e+4)-30] \text{ mai dacă } d+e+4 \geq 31$$

Care e primul an ≥ 2200 în care Pastele sunt. pînă pe 8 aprilie.