

Polinomane irreducibile si ideale maxime

Rezultatul (ans)

Prop  $K[\text{cpl}] \Rightarrow K[x]$  e ideal principial i.e. totu idealele sunt principiale

Idee  $I \subseteq K[x]$ . Aleg  $f \in I, f \neq 0, \deg f$  minim  $\overset{\text{D do maxima}}{\Rightarrow} I = (f)$ . Cu rest

Prop  $K[\text{cpl.}]$ .  $I \subseteq K[x], I = (f)$  e maxim  $\Leftrightarrow f$  irreducibil

$$\underline{\text{dvs}} \quad \left| \frac{K[x]}{(f)} \right| = p^n$$

$\uparrow$   
 $\deg f = n$

$$\frac{K(x)}{(f)} = \left\{ \overline{a_0 + a_1 x + \dots + a_{n-1} x^{n-1}} \mid a_i \in K \right\}$$

Cuadar  $f \in K[x]$  reducibil  $\Rightarrow K = \frac{K[x]}{(f)}$  e

cpl cu  $p^n$  elemente!

Iedera (anal II)  $\forall n \geq 1, \exists f \in K[x], \deg f = n, f$  reducibil.

Eac 2. Dacă că:

a)  $(x^2 - 2)$  maximal în  $\mathbb{Q}[x]$

Viz 1  $x^2 - 2$  ireducibil în  $\mathbb{Q}[x]$  pt că deg  $\leq 3$  și nu are roători în  $\mathbb{Q}$

$\Rightarrow (x^2 - 2)$  maximal

Viz 2  ~~$\mathbb{Q}(x)$~~   $\simeq \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Separate denotarea că  $\nearrow$  la copie!

$$(a + b\sqrt{2})^{-1} = \frac{(a - b\sqrt{2})}{a^2 - 2b^2}$$

$$\text{Max}(R) = \left\{ m \in R \mid m \text{ maximal} \right\}$$

c)  $(4, x) \notin \text{Max}(\mathbb{Z}[x])$

$2 \cdot 2 \in (4, x)$ , deci  $\hat{2} \cdot \hat{2} = \hat{0}$  în  $\frac{\mathbb{Z}[x]}{(4, x)}$ ,

dacă  $\hat{2} \neq \hat{0}$

$\Rightarrow \frac{\mathbb{Z}[x]}{(4, x)}$  nu este domeniu  $\Rightarrow$  nu e corp

Defapt,  $\frac{\mathbb{Z}[x]}{(4, x)} \stackrel{\text{Dito}}{\simeq} \frac{\mathbb{Z}[x]}{(4, x)} \xrightarrow{x \mapsto 0} \frac{\mathbb{Z}}{(4)} \simeq \mathbb{Z}_4$   
nu e corp

d)  $(2+i) \in \text{Max}(\mathbb{Z}[i])$

$\nearrow \text{irr. } \begin{matrix} \text{Lemn. 4-5-6.} \\ \sim \sim \end{matrix}$

nu e

a)  $\frac{\mathbb{K}[x]}{(2+x^2)} \stackrel{\text{Lemma 4.5.6?}}{\cong} \mathbb{K}_5$  eșig

e)  $(2, x^4+x^3+1) \in \text{Max}(\mathbb{K}[x])$

$$\frac{\mathbb{K}[x]}{(2, x^4+x^3+1)} \cong \frac{\mathbb{K}_2[x]}{(x^4+x^3+1)}$$

$x^4+x^3+1$  e rad în  $\mathbb{K}_2[x]$ .

Lulta de date teoreta:  $x^4+x^3+1$  este rad în  $\mathbb{K}_2[x]!$

3. Sunt următoarele ideale maxime în  $\mathbb{K}[x]$ ?

a)  $(5, x^3+2x^2+4x+3)$  nu

este rad  
 $\Rightarrow x^3+2x^2+4x+3$  e rad în  $\mathbb{K}_5[x]$ .

Dacă  $\hat{x}$  e rad a lui  $x^3+2x^2+4x+3$  în  $\mathbb{K}_5$   
 $\Rightarrow_{\text{def}}$  este redusibil!

b)  $(7, x^4+x^2+2) \in \text{Max}(\mathbb{K}[x]) \Rightarrow x^4+x^2+2$  e redusibil  
 în  $\mathbb{K}_7[x]$ .

Obs  $x^4+x^2+2$  nu are rădăcini în  $\mathbb{K}_7$

~~⇒~~ e redusibil (pt că se ghid  $4 > 3$ )

$\Rightarrow$  Dacă e redusibil,  $x^4+x^2+2 = P \cdot Q$ ,  $P, Q \in \mathbb{K}_7[x]$ ,

$\Rightarrow$  Sasaki reduction,  $x^4 + x^2 + 2 = f \cdot g$ ,  $Kg \in \mathbb{K}[x^3]$ ,  
 $\deg f = \deg g = 2$

$$x^4 + x^2 + 2 = x^4 - 6x^2 + 9 = (x^2 - 3)^2$$

Durch neu ordnen:  $x^4 + x^2 + 2 = (x^2 + ax + b)(x^2 + cx + d)$

$$\Rightarrow \begin{cases} bc = 2 \\ ad + bc = 0 \\ b + d + ac = 1 \\ a + c = 0 \end{cases} \quad \Rightarrow a = c = 0, b = d = -3 = 4$$

Ex 4 (Caterina Reducere)

Ex 4 (continuare)  $I \trianglelefteq R$ ,  $I \neq R$ . Dacă  $f \in R[X]$  monic este redusibil în  $R[X]$ .

Also  $\deg g, \deg h < \deg f$

$$\underline{\text{Defn 03}} \quad f = 1 \cdot x^n + a_{n-1}x^{n-1} + \dots - \quad (\text{fmonic})$$

$$q = q_0 \times l_1 \cdots$$

$$Q = c_l \times l$$

$$f_1, f_2, \dots, f_n : \Omega \rightarrow \mathbb{R} \text{ en } C^1(\Omega)$$

$$f = gh \Rightarrow \deg gh = 1 \Rightarrow g, h \in U(R)$$

$\underbrace{g, h \in U(R[x])}_{\deg g, \deg h \geq 1}$

R domnia:  $\deg f = \deg g + \deg h \Rightarrow \boxed{1 \leq \deg g, \deg h < n}$

Dec in  $(R/I)[x]$ :  $\bar{f} = \bar{g} \cdot \bar{h}$

$\deg n \quad \deg \bar{g} \leq \deg g < \deg f$   
(monic)

Prin ca  $\bar{g} \in U(R/I[x]) \Rightarrow \bar{g} \in \text{Ncl}(R/I)$

$\Rightarrow$  exist  $a \in \bar{g}^m \in I$

$\Downarrow$

$1 = \bar{g}^m \cdot c_l^m \in I \text{ do } I \neq R.$

Corolar ( $R = \mathbb{Z}$ )

Fie  $f \in \mathbb{Z}[x]$  monic. Daca  $f$  e deducibile in  $\mathbb{Z}_p[x]$   
 $\Rightarrow f$  e deducibile in  $\mathbb{Z}[x] \xrightarrow{\text{Lema Gauss}} \mathbb{Q}[x]$ .

Erc 5. Daca urmatoarele polinoame sunt deducibile:  
 a)  $x^5 + 9x^2 + 4x + 7 \in \mathbb{Z}[x]$

mc . . .

a)  $x^5 + 9x^2 + 4x + 7 \in \mathbb{Z}[x]$

b)  $x^4 - 3x^3 + 6x^2 - 2x + 1 \in \mathbb{Z}[x]$

c)  $x^2 + xy + 1 \in \mathbb{Z}[x, y]$

Denum a) Reducem în  $\mathbb{Z}_2$ :  $x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ .

Linia de date teoreta: este redusibil



$x^5 + 9x^2 + 4x + 7 \in \mathbb{Z}[x]$  este  
redusibil

Să vedem:  $x^5 + 20111x^2 - 66678x + 1 \in \mathbb{Z}[x]$   
este redusibil!

b) În  $\mathbb{Z}_3$ :  $x^4 + x + 1 \in \mathbb{Z}_3[x]$  are radacini!

În  $\mathbb{Z}_2$ :  $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$  + linia de date teoreta

c)  $\underline{x^2 + xy + 1} \in \mathbb{Z}[x, y].$

$\checkmark x^2 + xy + 1 \in \underbrace{\mathbb{Z}(Y)[x]}_{R \text{ din datele}} \text{ muncii}$

$\text{Dacă } I = (Y) \text{ și nu este polinom în } \left( \frac{\mathbb{Z}(Y)}{(Y)} \right)[x].$

Dacă  $x^2 + 1 \in \mathbb{Z}[x]$  este redusibil

"  
25x)



$$x^2 + xy + 1 \in \mathbb{Z}[x, y] \quad \text{---}$$

Teorema (detinută în Cech)

Dacă coeficienții unui polinom din  $\mathbb{Z}[x]$  sunt însele  
din scrierea într-o bază a unui număr prim, atunci  
polinomul este redusibil.

Fie  $b \in \mathbb{N}$ ,  $b \geq 2$  și  $p$  prim astfel

$$p = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0, \quad 0 \leq a_i < b$$

Astăzi  $f = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

este redusibil ( $\approx \mathbb{Z}[x]$  și  $\approx \mathbb{Q}[x]$ )

Eșantie 5471 e prim  $\xrightarrow[\text{în baza } 10]{\text{scriere}} 5x^3 + 4x^2 + 7x + 1$   
e redusibil.

179 prim  $\Rightarrow x^2 + 7x + 9$  e redusibil (baza 10)

$$179 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1$$

$$= (10110101)_2$$

$$\Rightarrow x^7 + x^5 + x^4 + x^2 + 1 \quad \text{reduzibel in } \mathbb{Z}[x] \text{ un. Q[x]}$$

$$179 = 1 \cdot 5^3 + 2 \cdot 5^2 + 0 \cdot 5^1 + 4 \cdot 5^0$$

$$= (1204)_5 \Rightarrow x^3 + 2x^2 + 4 \quad \text{red!}$$

Demonstratio gloria  $f = \sum_{i=0}^n a_i x^i$

Prüfen  $f = g \cdot h \mid (\beta)$   $p = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$

$$p = f(b) = g(b) \cdot h(b) \implies \underline{g(b) = \pm p} \quad \text{und} \quad \underline{h(b) = \pm p}$$

$$\hookrightarrow g = \sum_{i=0}^d c_i b^i, \quad d < n \quad \text{nu negat} \quad 0 \leq c_i < b$$

$$\underline{\pm p} = g(b) = \cancel{c_d b^d} + \cancel{c_{d-1} b^{d-1}} + \dots + \cancel{c_1 b} + \cancel{c_0}$$

~~No~~ an ungerades Radizier in Least b!

Ex 7 Prüfen auf Reduzibilität:

$$\text{a)} \quad x^6 + x^4 + x^3 + 1 : b=2 \Rightarrow 2^6 + 2^4 + 2^3 + 1 = 64 + 16 + 8 + 1 = 89 \quad \text{prim!}$$

$$\text{b)} \quad x^5 + x^4 + 2x + 1 : b=3 \Rightarrow 3^5 + 3^4 + 2 \cdot 3 + 1 = 243 + 81 + 6 + 1 = 331 \quad \text{prim!}$$

$$\text{c)} \quad 2x^3 + 5x^2 + 5x + 7 : b=10 \quad 2557 \quad \text{prim!}$$

c)  $2x^3 + 5x^2 + 5x + 7 : k=10 \cdot 2557$  über!

Ex 8  $K$  Körper,  $f \in K[x]$ . Welche Ideale bei  $\frac{K[x]}{(f)}$ ?  
Wieviel sind es?

Bem  $I$  der zugehörige:  $I \trianglelefteq \frac{K[x]}{(f)} \iff$

$$\iff I = \frac{I}{(f)}, \quad I \supset (f).$$

Da  $K[x]$  principal  $\Rightarrow I \trianglelefteq K[x], \quad I = (g)$  mit  $g \in K[x]$ .

$$\Rightarrow \left\{ \text{Ideale bei } \frac{K[x]}{(f)} \right\} = \left\{ \frac{(g)}{(f)} \mid (g) \supset (f) \Leftrightarrow g | f \right\}$$

Für  $f = f_1^{r_1} f_2^{r_2} \cdots f_k^{r_k}$  dekomponieren bei  $f$  in  
Faktoren der primären Reduzibilität

$$g | f \Rightarrow g = f_1^{l_1} f_2^{l_2} \cdots f_k^{l_k}, \quad l_j \leq r_j$$

$$\Rightarrow \left\{ \text{Ideale bei } \frac{K[x]}{(f)} \right\} = \left\{ \frac{(f_1^{l_1} f_2^{l_2} \cdots f_k^{l_k})}{(f)} \mid l_j \leq r_j \right\}$$

$$\text{Max } \left\{ \frac{(f_j)}{(f)} \mid 1 \leq j \leq k \right\}$$

Example  $\left\{ \text{Ideale bei } \frac{\mathbb{Q}[x]}{(x^3 - 1)} \right\} =$   
 $\dots, (x^2 + x + 1), (x^3 - 1), (1).$

$$= \left\{ \frac{(x-1)}{\cancel{(x^3-1)}}, \frac{(x^2+x+1)}{\cancel{(x^3-1)}}, \frac{(x^3-1)}{(x^3-1)}, \frac{(1)}{\cancel{(x^3-1)}} \right\}$$

*minimale*

Ques  $K[x]/(f)$  und local  $\Leftrightarrow f = h^m$ ,  $h$  reduzibel;  
 dann ist  $\text{Max}(K[x]/(f)) = \left\{ \frac{(h)}{(f)} \right\}$

Exerc 9 Herdete idealele lin  $\cancel{Z(x)}$  . Prezinta

Alle Jahre die rent maximale.

$$\underline{\text{Dear Anna}}$$

$$\frac{\mathbb{Z}[x]}{(2, x^3 + 1)} \cong \frac{\mathbb{Z}_2[x]}{(x^3 + 1)}$$

$$x^3 + 1 = (x+1)(x^2+x+1)$$

$\Rightarrow$  Ideale im  $\frac{\mathbb{Z}_2[x]}{(x^3+1)}$

descompõe-se em  $\mathbb{K}[x]$

$$(0), \quad \begin{array}{c} (x+i) \\ \diagup \\ (x^3+i) \end{array}, \quad \begin{array}{c} (x^2+x+i) \\ \diagup \\ (x^3+i) \end{array}$$

$$\mathcal{Z}[x]$$

$$\cancel{(2, x+1)}$$

$$\cancel{(2, x^2+x+1)} = \frac{(2, x^2-x+1)}{(2, x^3+1)}$$

127/14

12

12

$$\begin{array}{c}
 \begin{array}{ccc}
 \cancel{12} & 12 & 11 \\
 \cancel{\frac{2x^2}{(2)}} & \cancel{\frac{(2, x+1)}{(2)}} & \cancel{\frac{(2, x^2+x+1)}{(2)}} \\
 \cancel{\frac{(2, x^3+1)}{(2)}} & \cancel{\frac{(2, x^3+1)}{(2)}} & \cancel{\frac{(2, x^3+1)}{(2)}}
 \end{array}
 \\[10pt]
 \begin{array}{ccc}
 12 & 12 & 11 \\
 \cancel{\frac{f(x)}{(x+1)}} & \cancel{\frac{(x+1)}{(x^3+1)}} & \cancel{\frac{x^2+x+1}{(x^3+1)}}
 \end{array}
 \\[10pt]
 \begin{array}{ccc}
 11 & 11 & 11 \\
 \cancel{\frac{Z_2[x]}{(x+1) \cdot (x^3+x+1)}} & \cancel{\frac{(x+1)}{(x+1)(x^2+x+1)}}
 \end{array}
 \\[10pt]
 \begin{array}{ccc}
 12 LCR & & 
 \end{array}
 \end{array}$$

$\Rightarrow$

$\frac{Z_2[x]}{(x+1)(x^2+x+1)}$

$\frac{Z_2 \times Z_2[x]}{(x^2+x+1)}$

$\uparrow$   
 poly in  $Z_2$   
 elem

$\uparrow$   
 poly in  $\mathbb{F}_4$   
 elem

---

10.  $\text{Mat}(\mathbb{R}[x]) = ?$

$\left\{ (Q) \mid Q \in \mathbb{R}[x] \text{ reduplicable} \right\}$

$\{(f) \mid f \in \mathbb{R}[X] \text{ redusibil}\}$

Care sunt poli red. în  $\mathbb{R}[X]$ ?

• de grad 1:  $x-a$ ,  $a \in \mathbb{R}$

• de grad 2, fără rădăcini:  $x^2+bx+c$ ,  $\Delta = b^2 - 4c < 0$

• de grad  $\geq 3$ , fără rădăcini?

Fie  $f \in \mathbb{R}[X]$ ,  $\deg f \geq 3$ , fără rădăcini reale.

$f \in \mathbb{C}[X]$  se descompune în factori liniali (Teorema fundamentală a Algebrai)

$$\text{Dacă } f(z) = 0 \Rightarrow f(\bar{z}) = 0$$

$$f = \sum_{k=0}^n a_k z^k \quad . \quad f(z) = 0$$

$$\sum_{k=0}^n a_k z^k$$

$$\text{Conjugat: } 0 = \overline{f(z)} = \sum_{k=0}^n \overline{a_k} \bar{z}^k = \sum_{k=0}^n a_k \bar{z}^k = f(\bar{z})$$

$\Rightarrow f \in \mathbb{C}[X]$  de rădăcini de tipul  $z_1, \bar{z}_1, z_2, \bar{z}_2, \dots$   
cu multiplicitate  $m_1, m_2, \dots$

$$f = (x-z_1)(x-\bar{z}_1)(x-z_2)(x-\bar{z}_2) \dots$$

$$f = \underbrace{(x - z_1)(x - \bar{z}_1)}_{\substack{\parallel \\ \frac{1}{2} \operatorname{Re} z_1}} \underbrace{(x - z_2)(x - \bar{z}_2)}_{\substack{\parallel \\ |z_2|^2}} \dots$$

$$(x^2 - (z_1 + \bar{z}_1)x + z_1 \bar{z}_1) \in \mathbb{R}[x]$$

$\Rightarrow f$  nu este redusibil

Molala

Polinom redusibil în  $\mathbb{R}[x]$ :  $x-a$ ,  $a \in \mathbb{R}$   
 $x^2 + bx + c$ ,  $b^2 - 4c < 0$

Ex 11 \*\*\* Determinate ideale maxime în  $\mathbb{R}[X, Y]$ .

Puteți folosi ca ideale maxime în  $\mathbb{C}[X, Y]$  sunt  $(X-a, Y-b)$ ,  $a, b \in \mathbb{C}$ .

Exemplu

$$(X-a, Y-b), a, b \in \mathbb{R}$$

$$(X-a, Y^2 + bY + c), a, b, c \in \mathbb{R}, b^2 - 4c < 0$$

$$\begin{array}{ccc} (\mathbb{R}[X, Y]) & \simeq & (\mathbb{R}[Y]) \\ (X-a, Y^2 + bY + c) & & \vdash (Y^2 + bY + c) \end{array} \simeq \mathbb{C}.$$

Ex 12 Fixe  $R = \{f \in \mathbb{R}[X] \mid f(0) \in \mathbb{Q}\}$  și  $I = \{f \in R \mid f(0) = 0\}$ .  
D. d. m.

Exk 12 Für  $R = \{f \in \mathbb{R}(X) \mid f(0) \in \mathbb{Q}\}$  ist  $\mathbb{R} \subseteq R$   
 Da es Reste sind, da  $I \trianglelefteq R$  in  $\mathbb{Q}$  nicht gegeben!

Den  $I = (x)$ ? **NU**

$I = (x) \Leftrightarrow \forall f \in I, \exists g \in R \text{ ai } f = gx$   
 auf der grad  $\geq 1 \in \mathbb{Q}$ !

$$(x) = \{f \in R \mid f(0) = 0 \text{ ai teuerst degrad } 1 \in \mathbb{Q}\}$$

Da es  $I = (f_1, \dots, f_m)$ ,  $f_i \in \mathbb{I}$  da  $f_i(0) = 0$ .

$\Rightarrow \forall g \in I, \exists g_1, \dots, g_n \in R$  ai  $g = g_1 f_1 + \dots + g_m f_m$

$\Rightarrow$  grad  $\geq 1$  (nicht  $h^1$  teuerst degrad 1 al kein  $h$ ):

$$\rightarrow g^1 = g_1(0) \cdot f_1^1 + g_2(0) \cdot f_2^1 + \dots + g_m(0) f_m^1$$

↑                      ↓                      ↑  
 rechte fiktive       $\mathbb{Q}$                        $\mathbb{Q}$

dim  $\mathbb{R}$

$$\Rightarrow \mathbb{P} = \langle f_1^1, f_2^1, \dots, f_m^1 \rangle_{\mathbb{Q}}$$

$$\dim_{\mathbb{Q}} \mathbb{P} = \infty \quad (\mathbb{P} \text{ ist } \underline{\text{nennmässig!}})$$

$$(\text{da } \dim_{\mathbb{Q}} \mathbb{A}^n = n)$$

$\forall$  (daca  $\dim_{\mathbb{Q}} V < \infty \Rightarrow V \cong \mathbb{Q}^{\dim_{\mathbb{Q}} V} = \mathbb{Q}^n$ )

Ex 13. Orice corp finit are  $p^m$  elemente, și prin  $m \geq 1$ .  
Dacă Fix  $K$ .  $\dim K = p$  plin.

Or că  $q \mid |K|$ ,  $q \neq p \Rightarrow \exists a \in (K, +)$  astfel încât  $qa = 0$ .

$a \neq 0 \Rightarrow q = 0 \Rightarrow p \mid q$

Vac 2 Fix  $\varphi: \mathbb{Z} \rightarrow K$ ,  $\varphi(n) = \underbrace{1+1+\dots+1}_{n \text{ ori}}$ .

$\ker \varphi = \begin{cases} (0), \quad \dim K = 0 \Rightarrow \mathbb{Z} \hookrightarrow K \Rightarrow \mathbb{Q} \hookrightarrow K \text{ subcplp} \\ (p), \quad \dim K = p \Rightarrow \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \text{Im } \varphi \end{cases}$

$\Rightarrow \mathbb{Z}_p \subset K$  subcplp

$\Rightarrow K$  este  $\mathbb{Z}_p$ -extensie reală  $\stackrel{\text{definit}}{\Rightarrow} |K| = p^{\dim_{\mathbb{Z}_p} K} = p^n$ .

Teorema (anal II) Există, prin lemea izomorfism, un unic  
 cplp cu  $p^n$  elemente.

$\mathbb{Q}$        $\mathbb{Z}/p\mathbb{Z}$  -       $\mathbb{Z}_p[x]$        $\text{nu cplp!}$

Exercițiu  $\mathbb{Z}_2[x]$   $\xrightarrow{(x^3+x+1)}$   $\mathbb{Z}_2[x]$   $\xrightarrow{(x^3+x^2+1)}$  nu (căci) izomorf.

Din  $x^3+x+1$  și  $x^3+x^2+1$  sunt divizibile  
 $\Rightarrow$  căci cu  $2^3=8$  elemente

## Anul II Liniarizare

Anul I Idee: Dacă găsim  $\varphi: \mathbb{Z}_2[x] \xrightarrow{\sim} \mathbb{Z}_2[x]$  izomorfism de polinoame astfel încât  $\varphi(x^3+x+1) = x^3+x^2+1$ , am terminat:

$$\mathbb{Z}_2[x] \xrightarrow{(x^3+x+1)} \mathbb{Z}_2[x] \xrightarrow{\varphi} \mathbb{Z}_2[x] \xrightarrow{(x^3+x^2+1)}$$

Inversare  $R(a_n x^n + \dots + a_1 x + a_0) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$

Dată reprezentare:  $f$  red ( $\Leftrightarrow R(f)$ ) divizibilă

$$R(x^3+x+1) = x^3+x^2+1$$

$$R(a_n x^n + \dots + a_1 x + a_0)$$

Dacă  $R$  (izomorfism de niște?)

$$= x^n \left( a_n \frac{1}{x^n} + a_{n-1} \frac{1}{x^{n-1}} + \dots + a_1 \frac{1}{x} + a_0 \right)$$

$$R(f) = X^n f\left(\frac{1}{X}\right)$$

$$\deg f = n$$

$$\begin{matrix} X+1 & & 1 \\ || & & || \\ 1 & & 1 \end{matrix}$$

$$R(f+g) = R(f) + R(g): R(X^2+X) \neq R(X^2) + R(X)$$

$$R(f+g) \stackrel{?}{=} R(f) + R(g) : R(x^2+x) \neq R(x^2) + R(x)$$

$$R(f \cdot g) \stackrel{?}{=} R(f) \cdot R(g)$$

Obs  $R \circ R \neq R!$

$$\text{Für } \varphi \ (f(x) = f(x+i))$$

$$x^3 + x + i \mapsto (x+i)^3 + (x+i) + i = x^3 + x^2 - ix + i \\ -ix + i^2 + i = x^3 + x^2 + i$$

$\varphi$  evident izomorphismus ( $\in \mathbb{K}[x]$ ,  $\varphi^{-1} = \varphi$ )

Ex 15 Konstrukte Körpern an: 8, 27, ~~65~~, 49, 125 de Elemente. *mit Integrität!*

Cant corp cu  $p^n$  elemente  $\Leftrightarrow$  cant polini de grad  $n$   
reducibile  $\in \mathbb{K}_p[x]$

$$8 = 2^3 : x^3 + x + i \rightarrow K = \frac{\mathbb{K}_2[x]}{(x^3 + x + i)}$$

$$27 = 3^3 : x^3 - x + i \text{ nu are rad} \Rightarrow \text{irred} \rightarrow K = \frac{\mathbb{K}_3[x]}{(x^3 - x + i)}$$

$$49 = 7^2 : x^2 + i \text{ nu are rad} \Rightarrow \text{irred} \rightarrow K = \frac{\mathbb{K}_7[x]}{(x^2 + i)}$$

$$125 = 5^3 : x^3 + x + i \quad \Rightarrow K = \frac{\mathbb{K}_5[x]}{(x^3 + x + i)}$$

Exercițiu 16. să găsim și  $f = x^n - x + 1 \in \mathbb{K}_p[x]$ .

a) Arătăți că  $f$  nu are rădăcini în  $\mathbb{K}_p$ .

Denumit:  $a^p \equiv a \pmod{p}$

$$\Rightarrow f(\hat{a}) = \hat{a} - \hat{a} + 1 = 1 \neq 0, \quad \forall \hat{a} \in \mathbb{K}_p.$$

b) Arătăți că, dacă  $f$  are o rădăcină între -m și  $m$  în  $\mathbb{K}_p$ , atunci  $f$  are toate rădăcinile în  $\mathbb{K}_p$ .

Fie  $L$  corpul cu  $\lambda \in L$  și  $f(\lambda) = 0$ .

$\mathbb{K}_p^\times$

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

$$f(\lambda+1) = (\lambda+1)^n - (\lambda+1) + 1 \stackrel{\text{dak } n=1}{=} \lambda^n + \lambda^{n-1} - \lambda - 1 + 1 = \lambda^n - \lambda + 1 = f(\lambda) = 0.$$

Iată  $\lambda, \lambda+1, \lambda+2, \dots, \lambda+(p-1)$  sunt rădăcinile lui  $f$ !

$$f(\lambda+a) = (\lambda+a)^n - (\lambda+a) + 1 = \lambda^n + a\lambda^{n-1} - \lambda - a + 1 = \lambda^n - \lambda + 1 = 0.$$

c) Arătăți că  $f$  este redusibilă în  $\mathbb{K}_p[x]$ .

Op că  $f = gh \in \mathbb{K}_p[x]$ ,  $\deg g, \deg h < \deg f$ .

Într-un corp  $L \supset \mathbb{K}_p$ ,  $f$  are rădăcinile  $\lambda, \lambda+1, \dots, \lambda+(p-1)$ .

Int - m corz  $L \supseteq \mathbb{Z}_p$ , f are radacmle  $\alpha, \alpha^{+1}, \dots, \alpha^{+l} \alpha^{-1}$ .

$\Rightarrow g$  ale radacmle  $\alpha^{+i_1}, \alpha^{+i_2}, \dots, \alpha^{+i_m}$   $m < p$ .

$\mathbb{Z}_p[x]$

$$\xrightarrow{\text{coeff } x^{m-1}} + \left[ (\alpha^{+i_1}) + (\alpha^{+i_2}) + \dots + (\alpha^{+i_m}) \right] \in \mathbb{Z}_p$$

$$\begin{aligned} & m\alpha + \underbrace{(i_1 + \dots + i_m)}_{\in \mathbb{Z}_p} \in \mathbb{Z}_p \\ & 0 \end{aligned} \quad \left. \begin{array}{l} \Rightarrow \alpha \in \mathbb{Z}_p \text{ ob} \\ \text{f m a rad in } \mathbb{Z}_p \end{array} \right.$$