

## Seminar 9

## Structuri Algebrice în Informatică

$$\begin{array}{ll} p \mid q_0 & \frac{P}{q} \in \{-\frac{5}{1}, -\frac{5}{1}, -1, 1\} \\ q \mid q_m & \end{array}$$

$$f(1) = -1 \neq 0$$

$$f(-5) = 5^4 - 3 \cdot 5^3 - 5 \neq 0$$

$$f(-1) = -7 \neq 0$$

$$f(5) \neq 0$$

f nu are rădăcini rationale, deci nu are factor de grad 2.

Pp. că f se scrie sub forma  $f \cdot g$ , grad 2,  $g, h \in \mathbb{Q}[x]$

dacă polinomul  $g$  este  $\in \mathbb{Z}[x]$

$$f(x) = (ax^2 + bx + c)(dx^2 + ex + m) \quad a, b, c, d, e, m$$

$$\text{deoarece } x^4 \text{ este } a \cdot d = 1 \Rightarrow (a, d) \in \{-1, -1, 1, 1\}$$

$$\text{deoarece } a=d=-1 \Rightarrow f(x) = (-x^2 + bx + c)(-x^2 + ex + m) = (-1)^2 (x^2 - bx + c)(x^2 - ex - m)$$

$$\text{Pp că } a=b=1$$

$$\text{deoarece } x^3 \text{ este } ab + bd = e + b = 3$$

$$\text{deoarece } x^2 \text{ este } am + be + cd = m + b + c = 0$$

$$\text{deoarece } x \text{ este } bm + ce = 0$$

$$\text{deoarece } x^0 \text{ este } cm = 5$$

$$c \cdot m = -5 \Rightarrow$$

$$1) c = -5$$

$$m = 1$$

$$\begin{cases} b - 5c = 0 \\ c + b = 3 \\ 1 + bc + 5 = 0 \end{cases} \Rightarrow c = \frac{1}{2} \notin \mathbb{Z}$$

$$2) c = 5 \quad \begin{cases} -b + 5c = 0 \\ 1 + b = 3 \\ -1 + bc + 5 = 0 \end{cases} \Rightarrow c = \frac{2}{5} \notin \mathbb{Z}$$

→ analog 2

$$3) c = -5$$

$$m = 5$$

$$4) c = 1$$

$$m = 5$$

nu putem descrie un polinom  
într-o formă g.h  $\Rightarrow$  f ireductibil  
în  $\mathbb{Q}[x]$

( sau ) Reducem toti coeficienții mod 2

$$f \in \mathbb{Z}[x] \rightsquigarrow f = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$$

Dacă f nu descrie în  $\mathbb{Z}[x]$ ,  $f(x) = g_1(x) \cdot g_2(x)$

pării unitate (monici)  $\rightarrow 2 \bmod 2 \quad f(x) =$

$$= \hat{g}_1(x) \cdot \hat{g}_2(x)$$

$$\mathbb{Z}_2[1] \quad \mathbb{Z}_2[2]$$

monici

Dacă  $x^4 + x^3 + 1$  e irred în  $\mathbb{Z}_2[x]$   $\Rightarrow$

$\Rightarrow$  f nu se descompune în  $\mathbb{Z}[x]$  deci nu e în

$\mathbb{Q}[x] \Rightarrow$  f ireductibil în  $\mathbb{Q}[x]$

În final  $A = \mathbb{Q}[x]/(x^2 + 1) \bmod x^4 + 1$  și fie  $u \in A$

$\in A$ .

\* Determinați dacă  $u$  este idempotent ( $u^2 = u$ ?)  
 -1) -  $u$  este inversabil în  $A$ , dacă și, găsiți  $u^{-1}$ .

$$ut = \widehat{2x-1} + \widehat{x+1} \Rightarrow u \text{ nu e idempot}$$

$$u \cdot v = I \Rightarrow v \cdot u = \frac{1}{3} \widehat{x} + \frac{1}{3} \cdot u = I \Rightarrow u \text{ e inversibil} \\ u^{-1} = \frac{1}{3} \widehat{x} + \frac{1}{3}$$

Exercițiu Fix  $A$  inel comutativ și  $a \in A$ .

Anotați că  $A[x]/(x-a) \cong A$  rezultă deoarece

$f: A_1 \rightarrow A_2$  morfism de inele  $\Rightarrow A_2/\ker f \cong \text{Im } f$

căci  $\ell: A[x] \rightarrow A$  morfismuri de inle

$$\text{cu } \ker \ell = (x-a)$$

$$\ell(x-a) = 0$$

$$\ell(f(x)) = f(a) \quad \text{evaluarea polinomului în } a.$$

$$\ell(x^3 - 2x + 1) = a^3 - 2a + 1$$

$\ell$  e morfism de inel (I)  $\ell(f_1 + f_2) =$

$$= \ell(f_1) + \ell(f_2)$$

$$\ell(f_1 \cdot f_2) = (f_1 \cdot f_2)(a) = f_1(a) \cdot f_2(a) =$$

$$= \ell(f_1) \cdot \ell(f_2)$$

$$(II) \quad \ell(f_1 \cdot f_2) = \ell(f_1) \cdot \ell(f_2)$$

$$\ell(f_1 \cdot f_2)(a) = (f_1 \cdot f_2)(a) = f_1(a) \cdot f_2(a) = \ell(f_1) \cdot \ell(f_2)$$

(III)  $\ell(n)=I, II, IV$ , dec feste morphism  
die inek

$\ell$  surjektiv: Fil aet  $\in A[x]$  polynom  
constant  $\ell(a)=a \in \text{Im } \ell \Rightarrow \text{Im } \ell = A$

in  $\ell$  mrs

$$\cdot \ker \ell = \{ f \in A[x] \mid \ell(f) = 0 \}$$

$$f(a) = 0 \quad \text{ausw} \quad \begin{matrix} \text{a root} \\ \in \end{matrix} \quad (x-a) \mid f(x) \quad f(x-a) \\ \text{and st. } f \quad g(x)$$

idealul generat de  $(x-a)g \in A[x] \in$

$$\text{e)} \quad f \in (x-a)$$

$$\text{Deci } \ker \ell = (x-a)$$

Folgernd T. F. iso inek  $A[x]/\ker \ell \cong$   
 $\text{Im } \ell \quad A[x]/(x-a) \cong A$  iso die inek

$$g \rightarrow g(a)$$

Exercitii Anotof  $\cong \mathbb{Z}[x]/(x^2+1) \cong$

$$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$$

Se optco-T. F. iso caut  $\ell : \mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$   
morphism care in  $\ker \ell = (x^2+1)$

$$\ell(f(x)) = f(i)$$

$$\ell(x^2+1) = 0$$

$$\ell(x) \cdot \ell(x) + \ell(1) = 0$$

$$\ell(x) = \pm i \quad 3/5$$

se  $\ell$  bin definito:  $f \in \mathbb{Z}[x]^J \Rightarrow f(i) \in \mathbb{Z}^J$  est morphisme de module  
 $\ell(f_1 + f_2)(i) = f_1(i) + f_2(i) =$   
 $= \ell(f_1) + \ell(f_2)$   
 $\ell(f_1 \cdot f_2)(i) = f_1(i) \cdot f_2(i) = \ell(f_1) \cdot$   
 $\ell(f)$   
 $\ell(1) = 1$   
 $\ell(a+bi) \in \mathbb{C}^J \text{ si } a, b \in \mathbb{Z}$   
 $\ell$  surj:  $\forall a+bi \in \mathbb{C}^J \exists f \in \mathbb{Z}[x]^J$  tel que  
 $\ell(f(a+bi)) = a+bi \Rightarrow \ell$  surj:  
 $\in \mathbb{Z}[x]^J$

$\ker \ell = \{f \in \mathbb{Z}[x]^J : \ell(f) = 0\} \text{ si } f(i) = 0$   
 $i \text{ est r\acute{e}el.}$

nt  $f(x-i)$  au r\acute{e}sultant  $R[x]$  ne  
 $\in \mathbb{Z}[x]^J$

$f \in R[x]$  avem  $f(i) = 0 \Leftrightarrow f(\bar{i}) = 0 \Rightarrow f(-i) = 0$   
 $f \in \mathbb{K}[x] \Leftrightarrow f(i) = f(-i) = 0 \Leftrightarrow x \mid f(x)$   
 $x^2 + 1 \mid f$ , deci  $\ker f = (x^2 + 1)$

$\in \mathbb{Q}[x] \supset \in \mathbb{Z}[x]^J$

Aplicam T.F. lao imeli:  $\mathbb{Z}[x]^J / \ker f \cong$

$\mathbb{Z}[x]^J / (x^2 + 1) \cong \mathbb{Z}^{J, 2}$  izade imeli

Am  $B$  multia es, pt:  $\ell: A[x]^J \rightarrow B$   
 $\ell(f(x)) = f(a)$  est un morphisme de  
 module numit "morph. de nomb". 3/5