

$A[x] \Rightarrow f(x) = a_0 + a_1 x + \dots + a_m x^m$  ( $a_0, a_1, \dots, a_m$  s.m. coeficienți polin.)  
 $\text{grad}(f) = \text{cel mai mare număr natural } k \text{ a.i. } a_k \neq 0$   
 $\text{dacă } f(x) \neq 0 \quad \text{atunci } \text{grad}(0) \stackrel{\text{def}}{=} -\infty.$

Exemplu

$$f(x) = (-2x^6 + 7x^{2022}) \quad \text{grad}(f) = 2022$$

$$f(x) = 1 + 2x + 3x^2 + 0 \cdot x^3 + 0 \cdot x^4 + \dots + 0 \cdot x^{2022} = 1 + 2x + 3x^2 \quad \text{grad}(f_n) = 2$$

Notatie Dacă  $f(x) = a_0 + a_1 x + \dots + a_m x^m$  și  $a_m \neq 0$ , atunci  $\text{grad}(f) = m$   
 și  $a_m$  s.m. coeficientul dominant al polinomului  $f(x)$ .

Proprietăți ale lui  $(A[x], +, \cdot)$ :

$$\text{① } f, g \in A[x] \setminus \{0\} \Rightarrow \begin{aligned} \text{grad}(f+g) &\leq \max\{\text{grad}(f), \text{grad}(g)\} \\ \text{grad}(f \cdot g) &\leq \text{grad}(f) + \text{grad}(g) \end{aligned}$$

Ex:  $f, g \in \mathbb{Z}_4[x]$   $f(x) = \hat{2} + \hat{2}x + \hat{2}x^2$   $g(x) = \hat{3} + \hat{2}x$   
 $\text{grad}(f) = 2, \text{grad}(g) = 1$   $f(x) \cdot g(x) = \underbrace{\hat{6} + \hat{6}x + \hat{6}x^2}_{\text{grad}(f \cdot g) = 2} \leq \text{grad}(f) + \text{grad}(g)$

= are loc dacă și numai dacă produsul coeficienților  
 dominanți este  $\neq 0$ .  
 ②  $0_{A[x]} = 0$  (polinomul identic nul)  
 $1_{A[x]} = 1 = \underbrace{1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^m}_{a+0 \cdot x + \dots + 0 \cdot x^m = a} \in A[x] (\exists a \in A)$

NOTAȚIE: De acum înainte  $(A, +, \cdot)$  împărtășește proprietăți de bază (comutativitate, existența elementului neutru și existența elementelor inverse).

Def. Fix  $A$  un inel (com). Un element  $a \in A$  s.m.  
 divizor al lui zero dacă există  $x \in A$ ,  $x \neq 0$  a.i.  $a \cdot x = 0$ .  
 • În orice inel (nemul)  $0$  este divizor al lui zero ( $0 \cdot 1 = 0$ )

Reguli de calcul într-un inel

- 1)  $0 \cdot a = a \cdot 0 = 0 \Leftrightarrow a \in A$
- 2)  $a \cdot (-b) = (-a) \cdot b = -ab \Leftrightarrow a, b \in A$

.. un element inversabil nu e divizor al lui zero ( $\Rightarrow$  nu e divizor al lui zero) Dacă:  $a \in U(A) \stackrel{\text{def}}{\Leftrightarrow} \exists b \in A \text{ a.i. } a \cdot b = 1$

Dc. a este divizor al lui zero  $\Rightarrow (\exists) c \in A, c \neq 0$  s.t.  $a \cdot c = 0$

$$\begin{array}{l} (b \cdot a) \cdot c = 1 \cdot c = c \\ \parallel \\ b \cdot (a \cdot c) = b \cdot 0 = 0 \end{array} \Rightarrow c = 0 \Rightarrow$$

a nu este divizor al lui zero

P*?*

Notatie  $A$  inel  $\rightarrow D(A)$  multimea divizorilor lui.

Def Un inel  $A$  cu  $D(A) = \{0\}$  s.m. domeniu de integritate

(com) reciproc nu e

Obs Un corp este domeniu de integritate; dar nu sunt adevărat. ( $\mathbb{Z}, \mathbb{Z}[i]$   $\rightarrow$  domeniu de integritate; dar nu sunt corpuri)

$$\boxed{a \cdot b = 0 \Rightarrow \begin{cases} a=0 \text{ sau } b=0 \\ a, b \in A \end{cases}}$$

Fie  $m \geq 2$   $\cup(\mathbb{Z}_m) = \{x \mid 0 \leq x \leq m-1, (x, m) = 1\}$

$$D(\mathbb{Z}_m) = \mathbb{Z}_m \setminus \cup(\mathbb{Z}_m)$$

$D(\mathbb{Z}_m) = \mathbb{Z}_m \setminus \cup(\mathbb{Z}_m) \Leftrightarrow m$  e număr prim.

Exc 2! Fie  $m \geq 2$ .  $(\mathbb{Z}_m, +, \cdot)$  - corp  $\Leftrightarrow m$  e număr prim.

Def Fie  $A$  un inel. Atunci  $I$  submultime meridă ideal al lui  $A$  s.m. ideal al lui  $A$  dacă: 1)  $(I, +) \leq (A, +)$  2)  $a \cdot x \in I \quad \forall a \in A$   $\forall x \in A$

Obs ① Idealele lui  $(\mathbb{Z}, +, \cdot)$  sunt  $n\mathbb{Z}$ .

② Un inel  $(A, +, \cdot)$  are 2 ideale:  $\{0\}$  și  $A$ .

③ Exc! Un inel (număr)  $A$  este corp  $\Leftrightarrow A$  are exact 2 ideale.

(Dem: "  $\Rightarrow$  "  $A$  e corp. Fie  $I \neq \{0\}$  un ideal al lui  $A$ .

$\Rightarrow (\exists) x \in I, x \neq 0 \Rightarrow x \in \cup(A)$

Dar  $\boxed{x \in \cup(A) \quad x \in I \quad \text{Excl} \Rightarrow I = A}$

Dem Fie  $a \in A$ ;  $x \in \cup(A)$   
 $\Rightarrow (\exists) y \in A$  s.t.  $x \cdot y = 1$ .  
 $I$  e ideal  $\Rightarrow x \cdot (ya) \in I$

$$(xy) \cdot a = 1 \cdot a = a \Rightarrow a \in I \Rightarrow A \subseteq I \Rightarrow A = I$$

" $\Leftarrow$ " Fie  $a \in A, a \neq 0$ .  $\{ax \mid x \in A\}$  este un ideal al lui  $A$  (verifică i) și ii) def

$$a \cdot 1 = a \neq 0$$

ipoteza  $\Rightarrow \{ax \mid x \in A\} = A \ni 1 \Rightarrow 1 = a \cdot y \text{ pt un } y \in A \Rightarrow$   
 $\Rightarrow a \in U(A) \Rightarrow U(A) = A \setminus \{0\} \Rightarrow A \text{ e corp.}$

Operări cu ideale: ① Fie  $I, J$  ideale ale lui  $A$ . Atunci  $I \cap J$  și  $I + J$  sunt ideale ale lui  $A$ , unde  $I + J = \{ab \mid a \in I, b \in J\}$

(Exc!) (verifică def.)

② Dc.  $I, J$  sunt ideale ale lui  $A$  atunci  $I \cup J$  este ideal

Exc!

$I \subseteq J \text{ sau } J \subseteq I$ .

Pp. abs. că  $I \neq J$  și  $J \neq I \Rightarrow (\exists) x_1 \in I \setminus J \text{ și } (\exists) x_2 \in J \setminus I$

$I \cup J$  e ideal  $\Rightarrow x_1 + x_2 \in I \cup J \Rightarrow$

$x_1 + x_2 \in I$  și  $x_1 + x_2 \in J$

$x_1, x_2 \in I \cup J$

$(I + J) \subseteq (A + J)$

$x_1 \in I$        $x_2 \in J$

$(x_1 + x_2) - x_1 \in I \Rightarrow x_2 \in I$   $\text{doar } (x_2 \in J)$

1)  $x_1 + x_2 \in I$       2)  $x_1 + x_2 \in J$  duce la o contradicție.  $\Rightarrow$  Pp e false

Analog se arată că 2) duce la o contradicție.

Evident.

Def 1) Fie  $(A, +, \cdot)$  un inel și  $a \in A$ . Idealul generat de  $a$  se notează cu  $(a)$  sau  $aA$  și reprezintă multimea  $\{ax \mid x \in A\}$ . Idealul principal generat de  $a \in A$  ( $aA$  se mai numește idealul  $a$ ) se notează cu  $(a_1, \dots, a_m)A$  și reprezintă multimea  $\{a_1, \dots, a_m\}$ .

2) Idealul generat de multimea  $(a_1, \dots, a_m)A$  și reprezintă multimea  $(a_1, \dots, a_m)A = \{a_1b_1 + \dots + a_mb_m \mid b_1, \dots, b_m \in A\}$ .

Aplicatie ① Calculați  $I = (3\mathbb{Z} + (5\mathbb{Z} \cap 7\mathbb{Z})) + (8\mathbb{Z} \cap 20\mathbb{Z})$  - ideal al lui  $\mathbb{Z}$

Cine e  $m$ ?

Exc!  $\begin{cases} a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z} \end{cases}$

(Seminar)

$(a, b) = \text{c.m.m.d.c}(a, b)$   
 $[a, b] = \text{c.m.m.m.c}(a, b)$

$$I = (3\mathbb{Z} + 35\mathbb{Z}) + 40\mathbb{Z} = \mathbb{Z} + 40\mathbb{Z} = \mathbb{Z}.$$

Def Dacă  $A$  și  $B$  sunt 2 inele, atunci produsul direct al celor 2 inele este inelul, notat  $(A \times B, +, \cdot)$ , definit pe produsul cartezian  $A \times B$  astfel:

$$(a, b) + (c, d) = (a+c, b+d)$$

(Excl! Să se verifice că este inel)

$$(a, b) \cdot (c, d) = (ac, b \cdot d)$$

Excl! Să se arate că idealele lui  $(A \times B, +, \cdot)$ , unde  $A \times B$  este produsul direct al inelilor  $A$  și  $B$ , sunt de forma  $I \times J$  cu  $I$  ideal al lui  $A$  și  $J$  ideal al lui  $B$ .

Def Fie  $A$  și  $B$  2 inele. O funcție  $f: A \rightarrow B$  s.u. morfism de inele dacă: ①  $f(x+y) = f(x) + f(y)$   $\forall x, y \in A$   
 (unitar)  $\nwarrow$

$$2) f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in A$$

$$3) f(1_A) = 1_B.$$

$\nwarrow$   $f_A(x) = x$  este morfismul identitate (Excl!)

Exemplu ①  $\lambda_A: A \rightarrow A$   $f(k) = k \cdot 1_A \quad \forall k \in \mathbb{Z}$  este morfism de inel,

②  $f: \mathbb{Z} \rightarrow A$  unde  $(A, +_1)$  este un inel carecăre.

unde  $(A, +_1)$  este un inel de la ① în  $\mathbb{Z}$ .  $\nearrow$

③ Nu există morfisme de inele de la ① în  $\mathbb{Z}_2$ ,  $f(a+bi) = ab$

④ (Excl!) Să se arate că este un morfism de inele.

este un morfism de inele. produsul lor direct.

⑤ Fie  $A, B$  2 inele și  $(A \times B, +, \cdot)$  produsul lor direct.

Fie  $P_A: A \times B \rightarrow A$   $P_A((a, b)) = a \quad \forall (a, b) \in A \times B$

Atunci  $P_A: A \times B \rightarrow A$   $P_A((a, b)) = a \quad \forall (a, b) \in A \times B$

sunt morfisme surjective de inele.

sunt morfisme surjective de inele.

este un morfism surjectiv de inele.

Def Un morfism de inele bijectiv s.u. izomorfism de inele.

## Prop de bază ale morfismelor de inele

- compunerea a 2 morfisme de inele este un morfism de inele
- inversul unui izomorfism de inele este tot un izomorfism de inele
- **Ex!** Dacă  $f: A \rightarrow B$  este un morfism de inele și  $a \in U(A)$  ⇒  $f(a) \in U(B)$ .

Inel factor Fie  $(A, +, \cdot)$  un inel și  $I$  un ideal al lui  $A$ .  
 $(I, +) \leq (A, +) \subset$  grup abelian ⇒  $(I, +)$  este subgrup normal al lui  $(A, +)$

⇒ Putem considera grupul factor  $(A/I, +)$   
 $(\hat{a} + \hat{b} = \hat{a+b} ; \hat{a} = \hat{b} \text{ în } A/I \Rightarrow a-b \in I)$   
Definim pe  $A/I$  operația de înmulțire astfel:  $\hat{a} \cdot \hat{b} = ab$   
(**Ex!** operația este bine definită) și  $(A/I, +, \cdot)$  este inel,  
numit **inelul factor al lui  $A$  modulo  $I$**

Prop Fie  $f: A \rightarrow B$  un morfism de inele.  
a) Dacă  $I$  este un ideal al lui  $B$  ⇒  $f^{-1}(I) = \{a \in A | f(a) \in I\}$  este un ideal al lui  $A$ . (în particular  $\text{Ker } f = f^{-1}(\{0_B\})$  este un ideal al lui  $A$ )  
b)  $\text{Ker } f$  este un ideal al lui  $A$  și  $f$  injectiv ( $\Rightarrow \text{Ker } f = \{0_A\}$ ).  
c)  $f(A)$  este inel (subinel al lui  $B$ ).

Teorema fundamentală de izomorfism pt inele Fie  $f: A \rightarrow B$  un morfism de inele. Atunci are loc izomorfismul de inele:  
 $A/\text{Ker } f \cong f(A) = \text{Im } f$ .  
Mai mult,  $F: A/\text{Ker } f \rightarrow \text{Im } f$   $F(\hat{a}) = f(a)$  este izom. de inele.

Corolar (Lema chineză a resturilor, LCR)  
 Fie  $m_1, m_2 \geq 2$  2 nr. întregi a.i.  $(m_1, m_2) = 1$ . Atunci  
 $\mathbb{Z}_{m_1 m_2} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  ↑ produsul direct al învelor

Obs Se poate generaliza la:  $m_1, \dots, m_r \geq 2$  întregi a.i.  
 $(m_i, m_j) = 1 \quad (\forall i \neq j)$ . Atunci  $\mathbb{Z}_{m_1 \cdots m_r} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ .

Aplicatie practica  
 (Vezi Exc! seminat)

Calcoul solutiei  
 si  
 algoritmic

Sistemul de congruențe

$$\left\{ \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{array} \right.$$

are solutie unica mod  $(m_1 m_2 \cdots m_n)$

$m_1 \cdots m_n \geq 2$   
 $(m_i, m_j) = 1$   
 $(\forall i \neq j)$