

Seminar 2.

- Înțeles în corpuri. -

- Def  $(R, +, \cdot)$  s.m. inel dc:

1)  $(R, +)$  grup ab.

2)  $(R, \cdot)$  semigrup

3) • distrib. fătă de  $+$   $\left\{ \begin{array}{l} x(y+z) = xy + xz \\ (y+z)x = yx + zx \end{array} \right. , \forall x, y, z \in R.$

- $(R, +, \cdot)$  s.m. inel cu unitate, dc. cîm plus.

$\exists 1 \in R$  a.s.  $\forall x \in R$ ,  $x \cdot 1 = 1 \cdot x$ .

- Dacă  $(R, +, \cdot)$  inel cu unitate,  $x \in R$

$x$  este inv. în  $R$  dc.  $\exists x^{-1} \in R$  a.i.  $x x^{-1} = x^{-1} x = 1$ .

- $a \in R$ ,  $a \neq 0$  s.m. divizor al lui zero dc.

$\exists b \in R$ ,  $b \neq 0$  a.s.  $a \cdot b = 0$  sau  $b \cdot a = 0$

- $(R, +, \cdot)$  inel com. cu unitate,  $0 \neq 1$ , fără divizori ai lui zero = dom. de integritate.

• Def  $(k, +, \cdot)$  s.m corp dacă:

- 1)  $(k, +)$  gr. ab.
- 2)  $(k, \cdot)$  este gr.
- 3) distrib. fctă de  $+$ .

sau

1)  $(k, +, \cdot)$  inel cu unitate

2)  $|k| \geq 2$ .

3)  $\forall x \in k, x \neq 0, \exists x^{-1} \in k$  a.i.  $xx^{-1} = x^{-1}x = 1$ .

• Obs 1) Corpurile NU au divizori ai lui zero

2)  $(k, +, \cdot)$  corp  $\iff$   $k$  el. de int.  
 $\iff$  in general

• Exemplu:

1)  $(\mathbb{Z}, +, \cdot)$  inel com. cu unitate,  $0 \neq 1$ .  
fără div. ai lui 0.  
el. de int.

NU e corp.

2)  $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$  corp. comutative  
fiecare subcorp în corpul lor.

3)  $\mathbb{Z}$  subinel în  $(\mathbb{C}, +, \cdot)$  care NU e subcorp.

3)  $(\mathbb{C}, +, \cdot)$  corp. com.  $\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$   
 IS

$$(\mathbb{R} \times \mathbb{R}, +, \cdot) \quad (a, b) + (a', b') = (a+a', b+b')$$

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b).$$

### Inelul claselor de resturi modulo n

• Fie  $n \in \mathbb{N}, n \geq 2, n\mathbb{Z} = \{nh \mid h \in \mathbb{Z}\}$ .

, Th. cimp. cu rest în  $\mathbb{Z}$ :

$\forall a, b \in \mathbb{Z}, b \neq 0, \exists! q, r \in \mathbb{Z}$  ai  $a = bq + r$

$$0 \leq r < |b|.$$

$$\mathbb{Z}_n = \{\overset{\wedge}{0}, \overset{\wedge}{1}, \dots, \overset{\wedge}{n-1}\}.$$

$\overset{\wedge}{0} \in n\mathbb{Z}$      $\overset{\wedge}{1} \in 1+n\mathbb{Z}$      $\overset{\wedge}{n-1} \in (n-1)+n\mathbb{Z}$ .

$$\overset{\wedge}{i} + \overset{\wedge}{j} = \overset{\wedge}{i+j}, \quad \overset{\wedge}{i} \cdot \overset{\wedge}{j} = \overset{\wedge}{i \cdot j}$$

$(\mathbb{Z}_n, +)$  grup. ab.     $\overset{\wedge}{0}$  el. n.     $-\overset{\wedge}{i} = \overset{\wedge}{-i}$ .

$(\mathbb{Z}_n, \cdot)$  monoid com.     $\overset{\wedge}{1}$  el. n.

$(\mathbb{Z}_n, +, \cdot)$  inel com., cu unitate,  $\overset{\wedge}{0} + \overset{\wedge}{1}$ .

$n=2$ ,  $(\mathbb{Z}_2 = \{0, 1\}, +, \cdot)$  corp. com.

$n=4$ ,  $\begin{matrix} 1 \\ 2 \\ 3 \\ 0 \end{matrix} \cdot \begin{matrix} 1 \\ 2 \\ 3 \\ 0 \end{matrix} = \begin{matrix} 1 \\ 0 \end{matrix} = 0$  în  $\mathbb{Z}_4$ .

$\Rightarrow (\mathbb{Z}_4, +, \cdot)$  nu este c.m.m.d.c. ai lui 0.

• Exercițiu: Fie  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $i \in \mathbb{Z}_n$ .

$i$  inv. în  $(\mathbb{Z}_n, +, \cdot) \Leftrightarrow$  c.m.m.d.c. ( $i; n$ ) = 1.

Soluție: Recăzentim  $a = b$  în  $\mathbb{Z}_n \Leftrightarrow n | a - b$ .

$a, b \in \mathbb{Z}$ ,  $(a; b) = 1 \Leftrightarrow$

$\exists m, n \in \mathbb{Z}$  cu  $ma + nb = 1$ .

" $\Rightarrow$ "  $i$  inv. în  $\mathbb{Z}_n \Rightarrow \exists j \in \mathbb{Z}_n$  cu  $i \cdot j = 1$

$\Rightarrow i \cdot j = 1 \Rightarrow n | ij - 1 \Rightarrow \exists k \in \mathbb{Z}$  cu

$nk = ij - 1 \Rightarrow ij + (-k) \cdot n = 1 \Rightarrow (i; n) = 1$

" $\Leftarrow$ "  $(i; n) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$  cu  $i \cdot a + n \cdot b = 1$ .

$\Rightarrow 1 = \overbrace{i \cdot a + n \cdot b}^{\substack{n \\ = 0}} = \overbrace{i \cdot a + \underbrace{n \cdot b}_{= 0}}^{\substack{n \\ = 0}} = i \cdot a = i \cdot a$

$\Rightarrow i$  inv. în  $\mathbb{Z}_n$  și  $i^{-1} = a$

$(\mathbb{Z}_m, +, \cdot)$  corp  $\Leftrightarrow 1, 2, \dots, \overset{\wedge}{m-1}$  inv. în  $\mathbb{Z}_m$

$\Leftrightarrow (1; m) = (2; m) = \dots = (m-1; m) = 1 \Leftrightarrow m$  prim.

• Atenție: Ecuatia  $2x = 2$  se rezolvă astfel:

- în  $(\mathbb{R}, +, \cdot)$ :  $2^{-1} | 2x = 2 \Rightarrow x = 1$ .

- în  $(\mathbb{Z}, +, \cdot)$ :  $2x = 2 \Leftrightarrow 2x - 2 = 0 \Leftrightarrow$   
 $2(x-1) = 0 \Rightarrow x-1 = 0 \Rightarrow x = 1$ .

- în  $(\mathbb{Z}_m, +, \cdot)$  cu  $\begin{cases} m \neq 2 \\ m \text{ prim} \end{cases}$ .  $\mathbb{Z} \text{ nu are div. cu lini zero}$   
se rezolvă la fel ca în  $(\mathbb{R}, +, \cdot)$ .

- în  $(\mathbb{Z}_4, +, \cdot)$ :

$$2 \cdot x = 2 \Rightarrow 2 \cdot x - 2 = 0 \Rightarrow 2(x-1) = 0 \Rightarrow$$
$$\Rightarrow x-1 \in \{0, 2\} \Rightarrow x \in \{1, 3\}.$$

## Înțelesul polinoamelor într-o nedeterminată

- Fie  $(R, +, \cdot)$  inel com., cu unitate.

$$R[x] = \{f = a_0 + a_1x + \dots + a_nx^n \mid a_0, a_1, \dots, a_n \in R, n \in \mathbb{N}\}$$

- Dacă  $f, g \in R[x]$ ,

$$f = a_0 + a_1x + \dots + a_nx^n, \quad g = b_0 + b_1x + \dots + b_nx^n$$

$$f+g = (a_0+b_0) + (a_1+b_1)x + \dots + (a_n+b_n)x^n.$$

$\Rightarrow (R[x], +)$  grup abelian:

"+" asoc., com., 0 el. nul (polinomul nul)

$$-f = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

- Dacă  $f, g \in R[x]$ ,

$$f = a_0 + a_1x + \dots + a_nx^n, \quad g = b_0 + b_1x + \dots + b_nx^n$$

$$f \cdot g = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_nb_m x^{n+m}$$

folosim faptul că "+" este distrib. față de "+".

$\Rightarrow (R[x], \cdot)$  monoid com.

"+" asoc., com., 1 el. unitate

"·" este distrib. față de "+"

$\Rightarrow (R[x], +, \cdot)$  inel com. cu unitate

înțelesul polinoam. în nedet.  $X$  cu coef. în  $R$ .

## Gradul unui polinom

$\forall f \in R[x], f \neq 0$ , f admite o scriere unică de forma:  
 $f = a_0 + a_1 x + \dots + a_n x^n$ ,  $a_0, a_1, \dots, a_n \in R$ ,  $a_n \neq 0$  (1)

$$\text{grad } f = \begin{cases} -\infty, & f = 0 \\ n, & f \neq 0 \text{ dat de (1)} \end{cases}$$

Obs. 1)  $\text{grad } f = 0 \Leftrightarrow f = a_0 \neq 0 \Leftrightarrow f \in R^*$

(Polinoamele de grad 0 sunt constantele nenule.)

2)  $\text{grad}(f+g) \leq \max\{\text{grad } f, \text{grad } g\}$ .

3)  $\text{grad}(f \cdot g) \leq \text{grad } f + \text{grad } g$

$\hookrightarrow a_n \cdot b_m$  poate fi 0.

$$\text{Ex: } f = \hat{2}x \in \mathbb{K}_4[x] \Rightarrow g = \hat{2}x^2 + 1.$$

$$f \cdot g = \underset{\hat{0}}{\underset{\hat{0}}{\underset{\hat{0}}{\underset{\hat{0}}{}}}} x^3 + \hat{2}x = \hat{2}x \Rightarrow \text{grad}(fg) = 1$$

$$\text{dor } \text{grad } f + \text{grad } g = 1+2=3.$$

4) Dacă  $R$  dom. int  $\Rightarrow \text{grad}(f \cdot g) = \text{grad } f + \text{grad } g$ .

Exercițiu: Fie  $(k, +, \cdot)$  corp. comutativ. S.s.a.c.

a)  $(k[x], +, \cdot)$  dom. int

b)  $f \in k[x]$  el. inv  $\iff f \in k^*$  ( $f$  inversabil în  $k$ ).

Soluție:

a)  $k[x]$  imel com. cu unitate  $0 \neq 1$ , fără div. si lui 0?

$$f \cdot g = 0 \stackrel{?}{\Rightarrow} f = 0 \text{ sau } g = 0.$$

$$\text{grad}(f \cdot g) = -\infty$$

$$k \text{ corp} \Rightarrow k \text{ dom. int} \Rightarrow \text{grad}(f \cdot g) = \text{grad } f + \text{grad } g \quad \Rightarrow$$

$$\Rightarrow \text{grad } f = -\infty \text{ sau } \text{grad } g = -\infty \Rightarrow f = 0 \text{ sau } g = 0.$$

b) " $\Leftarrow$ " Evident.

" $\Rightarrow$ "  $f \in k[x]$  inversabil  $\Rightarrow \exists g \in k[x]$  aș  $f \cdot g = 1$ .

$$\Rightarrow \text{grad}(f \cdot g) = 0 \Rightarrow \text{grad}(f) + \text{grad}(g) = 0 \Rightarrow$$

$$\Rightarrow \text{grad } f = \text{grad } g = 0 \Rightarrow f \in k^*. (g \in k^*)$$

Th. împărțirii cu rest în  $k[x]$ :

$\forall f, g \in k[x], g \neq 0, \exists! q, r \in k[x]$  aș:

$$f = g \cdot q + r, \text{ cu } \text{grad } r < \text{grad } g$$