Algebră

- Seminar -

26.02.2018

Inele

$(R, *, \cdot)$

R - mulțime

$\left.\begin{matrix} * \\ \circ \end{matrix}\right\}$ operații alg

$(R, *, \circ)$ (Not $(R, +, \cdot)$) este inel dacă

1) $(R, *)$ grup comutativ

$\left\{\begin{matrix} 2) (R, \cdot) \text{ semigrup} \\ 2') (R, \cdot) \text{ monoid (pt inel unitar)} \end{matrix}\right.$

3) Distributivitate: $\forall a, b, c \in R$

$a \cdot (b+c) = a \cdot b + a \cdot c$

$(a+b) \cdot c = a \cdot c + b \cdot c$

$\mathcal{U}(R) = \{a \in R \mid \exists b \in R, \text{ a.î. } ab = ba = 1_R\}$

$\mathcal{U}(R)$ grupul unităților lui R

Ex 1 $M = \left\{\begin{pmatrix} a & b \\ \hat{0} & c \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_p\right\}$

$(M, +, \cdot)$ formează un inel unitar. Calc $\mathcal{U}(M)$

Rez $(M, +)$ gr. com.

+ p.s. în rap. cu M.

+ asoc (adunarea mat este asoc)

+ com (adun ~~com~~ mat este com)

$\bar{0} \in \mathbb{Z}_p \Rightarrow O_2 \in M$ el. neutru

$\forall \hat{a} \in \mathbb{Z}_p, \exists p-a \in \mathbb{Z}_p$ a.î. $p-a+a = p = \bar{0}$ în $\mathbb{Z}_p \Rightarrow$

$\Rightarrow \forall A \in M, \exists -A \in M$ a.î. $A + (-A) = (-A) + A = O_2$.

$\Bigg\}$ $(M, +)$ gr. com

$(M, \cdot)$ monoid

- asoc (înm mat este asoc)
- ps. față de M

$I_2 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} \in M$ – el. n

Înm mat este distrib față de adunarea lor.

$A \in U(M) \Rightarrow \exists B \in M$ a.î. $AB = BA = I_2$

$$\begin{pmatrix} \hat{a}_1 & \hat{a}_2 \\ \hat{0} & \hat{a}_3 \end{pmatrix}\begin{pmatrix} \hat{b}_1 & \hat{b}_2 \\ \hat{0} & \hat{b}_3 \end{pmatrix} = I_2 \Rightarrow$$

$$\Rightarrow \begin{pmatrix} \widehat{a_1 b_1} & \widehat{a_1 b_2 + a_2 b_3} \\ \hat{0} & \widehat{a_3 b_3} \end{pmatrix} = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} \Rightarrow$$

$\Rightarrow \widehat{a_1 b_1} = \hat{1}$

$\widehat{a_1 b_2 + a_2 b_3} = \hat{0}$

$\widehat{a_3 b_3} = \hat{1}$

Analog $BA = I_2 \Rightarrow$

$\Rightarrow \widehat{b_1 a_1} = \hat{1}$

$\widehat{b_1 a_2 + b_2 a_3} = \hat{0}$

$\widehat{b_3 a_3} = \hat{1}$

$$U(M) = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{0} & \hat{c} \end{pmatrix} \middle| \begin{array}{l} \hat{a} \in U(\mathbb{Z}_p) \\ \hat{c} \in U(\mathbb{Z}_p) \\ \exists \hat{b}_1, \hat{b}_2, \hat{b}_3 \in \mathbb{Z}_p \text{ a.î. } \widehat{a b_2} + \widehat{b b_3} = \hat{0} \\ \qquad \widehat{b_1 b} + \widehat{b_2 c} = \hat{0} \end{array} \right\}$$

$U(\mathbb{Z}_p) = \mathbb{Z}_p^*$

$U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$

Ex 2:

$\nearrow \langle \hat{1} \rangle \Rightarrow \hat{a} = \underbrace{\hat{1}+\hat{1}+\dots+\hat{1}}$

$(\mathbb{Z}_p, +)$ grup $(\mathbb{Z}_p, +, \cdot)$ inel

$*: \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ a.î. $(\mathbb{Z}_p, +, *)$ inel

$* = ?$

$\hat{a}, \hat{b} \in \mathbb{Z}_p$

$$\hat{a} * \hat{b} = \underbrace{(\hat{1}+\hat{1}+\dots+\hat{1})}_{\text{de } a \text{ ori}} * \hat{b} = \underbrace{\hat{1}*\hat{b} + \hat{1}*\hat{b} + \dots + \hat{1}*\hat{b}}_{\text{de } a \text{ ori}} = \cancel{\hat{1}*(\underbrace{\hat{1}+\dots+\hat{1}}_{\text{de } b \text{ ori}})}$$

$$= \underbrace{\hat{1} * \underbrace{(\hat{1}+\dots+\hat{1})}_{b \text{ elem}} + \dots + \hat{1}\underbrace{(\hat{1}+\dots+\hat{1})}_{b \text{ elem}}}_{a \text{ elem}} = \underbrace{\hat{1}*\hat{1} + \hat{1}*\hat{1} + \dots + \hat{1}*\hat{1}}_{a \cdot b \text{ elem.}} =$$

$$= a \cdot b \cdot (\hat{1} * \hat{1})$$

$*_a : \hat{x} *_a \hat{y} = \widehat{xya}$

$\hat{1} *_a \hat{1} = a$

$(\mathbb{Z}_p, +, *_a)$ inel; $\forall \hat{a} \in \mathbb{Z}_p \Rightarrow p$ inele cu $(\mathbb{Z}_p, +)$

$\cdot = *_1$

$$\boxed{(\mathbb{Z}_p, +, *_a) \overset{?}{\cong} (\mathbb{Z}_p, +, \cdot)}$$

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

- fct $f: R_1 \to R_2$ s.n. morfism de inele dacă
  1) $f(a+b) = f(a) + f(b)$
  2) $f(a \cdot b) = f(a) \cdot f(b)$

Dacă $f(1_{R_1}) = 1_{R_2}$, atunci f este morfism unitar.

f este fct bijectivă, atunci f se numește izomorfism

$f: (\mathbb{Z}_p, +, \cdot) \to (\mathbb{Z}_p, +, \cdot)$

$\hat{a} \in \mathbb{Z}_p$

$f(\hat{x}) = \widehat{ax}$

(1) $f(x+y) = f(x) + f(y)$

$f(x+y) = \widehat{a(x+y)} = \widehat{ax+ay} = f(x) + f(y)$

(2) $\cancel{f(x \cdot xy)}$ $f(x \cdot y) = f(x) f(y)$

$f(x \cdot y) = \widehat{a(x \cdot y)} =$

$= \widehat{a \cdot xy \cdot a}$

$= \widehat{a \cdot x}\ \widehat{y a} =$

$= f(x)\ f(y)$

(1) şi (2) $\Rightarrow$ f morfism

b)

$\cancel{x, y \quad f(x) = f(y) \Rightarrow x = y}$

$f(x) = f(y) \Leftrightarrow \widehat{ax} = \widehat{ay} \quad | \hat{a}^{-1}$

$\hat{a} \neq 0 \overset{p\ prim}{\Rightarrow} \exists\, \hat{a}^{-1} \in \mathbb{Z}_p$ a.î. $\hat{a} \cdot \hat{a}^{-1} = \hat{1} \Rightarrow x = y \Rightarrow f$ inj

$\cancel{\forall\, \hat{y} \in \mathbb{Z}_p \Rightarrow \exists\, x \in \mathbb{Z}_p \text{ a.î. } y}$

Fie $\hat{y} \in \mathbb{Z}_p$

$\hat{y} = \widehat{ax} \Rightarrow x = \hat{y}\hat{a}^{-1} \Rightarrow f$ surj

$\Rightarrow$

$\Rightarrow$ f izomorfism

$(\mathbb{Z}_p, +)$ $\begin{cases} (\mathbb{Z}_p, +, \cdot) \\ (\mathbb{Z}_p, +, *_0) \end{cases}$ 2 str. de inel neizomorfe

$$\forall \hat{x}, \hat{y} \in \mathbb{Z}_p, \ \hat{x} *_0 \hat{y} = \hat{0}$$

$\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +\right)$ – Există structură de inel unitar pe grupul $\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +\right)$?

$*: \frac{\mathbb{Q}}{\mathbb{Z}} \times \frac{\mathbb{Q}}{\mathbb{Z}} \to \frac{\mathbb{Q}}{\mathbb{Z}}$ op. alg a.î. $\left(\frac{\mathbb{Q}}{\mathbb{Z}}, +, *\right)$ inel unitar.

$\exists \ \widehat{\frac{m}{n}} \in \frac{\mathbb{Q}}{\mathbb{Z}}$ a.î. $\widehat{\frac{m}{n}} \cdot \hat{x} = \hat{x} \cdot \widehat{\frac{m}{n}} = \hat{x} \ (\forall) \hat{x} \in \frac{\mathbb{Q}}{\mathbb{Z}}$

$\widehat{\frac{m}{n}} = \hat{e}$

$$\widehat{\frac{1}{m}} = \widehat{\frac{1}{m}} \cdot \widehat{\frac{m}{n}} = \widehat{\frac{1}{m}} * \underbrace{\left(\widehat{\frac{1}{n}} + \widehat{\frac{1}{n}} + \dots + \widehat{\frac{1}{n}}\right)}_{m \text{ elem.}} = \underbrace{\widehat{\frac{1}{m}} * \widehat{\frac{1}{n}} + \dots + \widehat{\frac{1}{m}} * \widehat{\frac{1}{n}}}_{m \text{ elem.}} =$$

$m \neq 0$

$$= \underbrace{\left(\widehat{\frac{1}{m}} + \dots + \widehat{\frac{1}{m}}\right)}_{m \text{ elem}} \widehat{\frac{1}{n}} = \widehat{\frac{m}{m}} * \widehat{\frac{1}{n}} = \hat{1} * \widehat{\frac{1}{n}} = \hat{0} * \widehat{\frac{1}{n}} = \hat{0}$$

$1 \in \mathbb{Z} \Rightarrow \hat{1} = \hat{0}$

$\hat{1} = 1 + \mathbb{Z} = \{1 + a \mid a \in \mathbb{Z}\} = \{x \mid x \in \mathbb{Z}\} = \hat{0}$

$\widehat{\frac{1}{m}} = \hat{0} \Leftrightarrow \frac{1}{m} \in \mathbb{Z} \Rightarrow m \in \{\pm 1\}$

$$\widehat{\frac{n}{n+1}} = \widehat{\frac{1}{n}} * \widehat{\frac{n}{n+1}} = \widehat{\frac{1}{n}} * \underbrace{\left(\widehat{\frac{1}{n+1}} + \dots + \widehat{\frac{1}{n+1}}\right)}_{n \text{ elem}} = \underbrace{\widehat{\frac{1}{n}} * \widehat{\frac{1}{n+1}} + \dots + \widehat{\frac{1}{n}} * \widehat{\frac{1}{n+1}}}_{n \text{ elem}} =$$

$$= \underbrace{\left(\widehat{\frac{1}{n}} + \dots + \widehat{\frac{1}{n}}\right)}_{n \text{ elem}} * \widehat{\frac{1}{n+1}} = \widehat{\frac{n}{n}} * \widehat{\frac{1}{n+1}} = \hat{1} * \widehat{\frac{1}{n+1}} = \hat{0} * \widehat{\frac{1}{n+1}} = \hat{0}$$

$\widehat{\frac{n}{n+1}} = \hat{0} \Rightarrow \frac{n}{n+1} \in \mathbb{Z}$ fals.

Dacă $n = -2 \Rightarrow \frac{n}{n+1} = \frac{-2}{-1} = 2 \in \mathbb{Z}$

$n = -2 \Rightarrow \widehat{\frac{m}{n}} = \frac{\hat{-1}}{2} = \widehat{\left(-\frac{1}{2}+1\right)} = \frac{\hat{1}}{2}.$

$\frac{2}{2+1} = \frac{2}{3} \notin \mathbb{Z}$

Algebră

– Seminar –

<u>Def</u> $(R,+,\cdot)$ un inel și $a\in R$. a se numește divizor al lui zero în R la dreapta (resp. la stânga) dacă $\exists b\in R, b\neq 0$ a.î. $a\cdot b=0$ (~~resp~~ resp $b\cdot a=0$)

$D(R)$ = mulț. divizorilor lui zero ai lui R

<u>obs</u> a este divizor al lui 0 dacă a este divizor al lui zero la dreapta și la stânga.

<u>Def</u>: $D(R)=\{0\} \Rightarrow$ R s.n inel integru
R este inel comutativ $\Big| \Rightarrow$ R s.n domeniu de integritate

<u>Exp</u>: $(\mathbb{R},+,\cdot)$ inel integru, $\underbrace{(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{C},+,\cdot)}_{\text{inele integre}}$

<u>Ex</u> $(\mathcal{M}_2(\mathbb{R}),+,\cdot)$; $A=\begin{pmatrix}1&0\\0&0\end{pmatrix}$

$B=\begin{pmatrix}0&0\\y&z\end{pmatrix}$ $\Big| \Rightarrow AB=0_2$

~~Ex~~

1\. a) $(\mathbb{Z}_{30},+,\cdot)$

$D(\mathbb{Z}_{30})=\{\hat{2},\hat{15},\hat{6},\hat{5},\hat{3},\hat{10},\hat{0},\hat{12}\ldots\}=\{\hat{a}\in\mathbb{Z}_{30}\mid (a,30)\neq 1\}$

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

$D(\mathbb{Z}_n)=\{\hat{a}\in\mathbb{Z}_n \mid (a,n)\neq 1\}$

Ex

2. $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$

$(\mathbb{Z}[i],+,\cdot)$ este inel com?

Spac $(\mathbb{Z}[i],+,\cdot)$ dom de integritate
(inel)

$(a+ib)(c+id) = 0+0i \Rightarrow \begin{cases} ac-bd=0 \\ ad+bc=0 \end{cases}$

$(ac-bd)+i(ad+bc) = 0+0i$

$\Leftrightarrow ac = bd \Rightarrow \text{I } c = \frac{bd}{a}$ $a \neq 0$

I $a=0 \Rightarrow bd=0 \Rightarrow$ i) $b=0 \Rightarrow ad+bc=0$, $(a,b)=(0,0)$ $\nexists$ div de 0

I $a \neq 0 \Rightarrow$ $ad+bc = ad+b\frac{bd}{a} = 0 \Rightarrow$

$\Rightarrow a^2d+b^2d=0 \Rightarrow d(a^2+b^2)=0$ $a \neq 0 \Rightarrow$ $\Rightarrow a^2+b^2 \neq 0$ $\Rightarrow d=0 \Rightarrow \begin{cases} ac=0 \\ a\neq 0 \end{cases} \Rightarrow c=0 \Rightarrow$

$\Rightarrow (c,d)=(0,0) \Rightarrow c+id=0$ nu $\nexists$ div ai lui 0 (2)

(1) si (2) $\Rightarrow (\mathbb{Z}[i],+,\cdot)$ dom de integritate.

Def: $(R,+,\cdot)$ un inel si $a\in R$, a s.n nilpotent dacă $\exists k\in\mathbb{N}^*$ a.î. a^k

Exp: $(\mathbb{Z}_8,+,\cdot)$

$\hat{2}\in\mathbb{Z}_8$ e nilpotent $(\hat{2}^3=\hat{0})$

$(\mathbb{Z}_{12},+,\cdot)$

$\mathcal{N}(\mathbb{Z}_{12}) = \{\hat{0},\hat{6}\} = \hat{6}\,\mathbb{Z}_{12} = \{\hat{0},\hat{6}\}$

$12 = 2\cdot 3$

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

$\mathcal{N}(\mathbb{Z}_n) =$

$|\mathcal{N}($

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

$N(\mathbb{Z}_n) = \widehat{p_1 \cdots p_t}\, \mathbb{Z}_n = \{\hat{0}, \widehat{p_1 \cdots p_t}, \hat{2}\, \widehat{p_1 \cdots p_t}, \ldots, \widehat{(n-1)}\, \widehat{p_1 \cdots p_t}\}$

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$

$|N(\mathbb{Z}_n)| = \dfrac{n}{p_1 \cdots p_t}$

Def: $(R, +, \cdot)$ inel. și $a \in R$. a s.n idempotent dacă $a^2 = a$.

Obs $0 \in \mathrm{Idem}(R)$

$1 \in \mathrm{Idem}(R)$

$a^2 = a \Leftrightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0 \Rightarrow a \in D(R)$

$a - 1 \in D(R)$

Exp $(\mathbb{Z}_{12}, +, \cdot)$

$12 = 2^2 \cdot 3$

$(2, 3) = 1 \Rightarrow \exists\, \alpha, \beta$ a.î. $2\alpha + 3\beta = 1$

$\alpha = -1$
$\beta = 1$

Alg Euclid
$$\begin{cases} n \\ x \\ n = x \cdot q_0 \\ x = r_0 q_1 + r_1 \\ r_0 = r_1 q_2 + r_2 \\ r_{p-1} = r_p q_{p+1} + r_{p+1} \\ r_p = r_{p+1} q_{p+2} + r_{p+2} \\ r_{p+2} = 0 \Rightarrow (n, x) = r_{p+1} = 1 \end{cases}$$

$(4, 3) = 1,\ 4\alpha + 3\beta = 1$

$\alpha = 1$
$\beta = -1$

$\hat{x} = \widehat{4\alpha} = \hat{4}$

$\hat{4}^2 = \hat{4}$

$(\mathbb{Z}_n, +, \cdot)$, $n = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$

$|\mathrm{Idem}(\mathbb{Z}_n)| = |\mathcal{P}(\{p_1, \ldots, p_t\})| = 2^t$

$\{p_{i_1}, \ldots p_{i_k}\}$

$\{p_{j_1}, \ldots p_{j_{t-k}}\} = \{p_1, \ldots p_t\} \setminus \{p_{i_1}, \ldots, p_{i_k}\}$

$(p_{i_1}^{\alpha_{i_1}} \cdot \ldots p_{i_k}^{\alpha_{i_k}}, p_{j_1}^{\alpha_{j_1}} \cdot \ldots \cdot p_{j_{t-k}}^{\alpha_{j_{t-k}}}) = 1$

$\alpha\, p_{i_1}^{\alpha_{i_1}} \ldots p_{i_k}^{\alpha_{i_k}} + \beta\, p_{j_1}^{\alpha_{j_1}} \ldots p_{j_{t-k}}^{\alpha_{j_{t-k}}} = 1$

$\overbrace{\alpha\, p_{i_1}^{\alpha_{i_1}} \ldots p_{i_k}^{\alpha_{i_k}} (-1 + \alpha\, p_{i_1}^{\alpha_{i_1}} \ldots p_{i_k}^{\alpha_{i_k}})} = \overbrace{-\alpha\, p_{i_1}^{\alpha_{i_1}} \ldots p_{i_k}^{\alpha_{i_k}}\, \beta\, p_{j_1}^{\alpha_{j_1}} \ldots p_{j_k}^{\alpha_{j_k}}}$

$\widehat{-\alpha\beta n} = \hat{0}$

<u>Exp:</u> $\mathrm{Idem}(\mathbb{Z}_{36})$

$36 = 2^2 \cdot 3^2$

$\{2, 3\}$

$\{\emptyset, \{2\}, \{3\}, \{2,3\}\}$ $\hat{1} \in \mathrm{Idem}(\mathbb{Z}_{36})$

P1. $\emptyset \to \hat{x} = \hat{0} \Rightarrow \hat{0} \in \mathrm{Idem}(\mathbb{Z}_{36})$, 1

P2 $\{2\} \to \{\hat{3}\}$

$(2^2, 3^2) = (4, 9) = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z}$ a.î. $4\alpha + 9\beta = 1$

$\alpha = -2$

$\beta = 1$

$x = \widehat{-2 \cdot 4} =$

$\hat{x} = \widehat{-2 \cdot 4} = \widehat{-8} = \widehat{28} \in \mathrm{Idem}(\mathbb{Z}_{36})$

P3 $\{3\} \xrightarrow{\text{complem}} \{2\}$

$(3^2, 2^2) = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z}$ a.î. $9\alpha + 4\beta = 1$

$\alpha = 1$

$\beta = -2$

$x = \widehat{\alpha \cdot 3^2} = \widehat{1 \cdot 3^2} = \hat{9} \in \mathrm{Idem}(\mathbb{Z}_{36})$

Def: $(R,+,\cdot)$ inel, $S\subseteq R$ s.n. subinel al lui R dacă

$(S,+,\cdot)$ este inel

$\left(\begin{array}{l}\overbrace{a-b\in S}^{(S,+)\text{ subgrup}}\\ \underbrace{a\cdot b\in S}_{\text{parte stabilă}}\end{array} ;\forall a,b\in S\right)$

ex: $(\mathbb{Q},+,\cdot)$; $\mathbb{Z}_{(2)}=\{\frac{a}{b} \mid b \text{ impar}, a,b\in\mathbb{Z}\}$

$(\mathbb{Z}_{(2)},+,\cdot)$

$\frac{a}{b},\frac{x}{y}\in\mathbb{Z}_{(2)} \Rightarrow \frac{a}{b}-\frac{x}{y}=\frac{ay-bx}{by}$ ~~$\Rightarrow$~~

$\cancel{by}$ $\cancel{ay-bx}$

by impar

$\Rightarrow \frac{a}{b}-\frac{x}{y}\in\mathbb{Z}_{(2)}$

$\frac{a}{b}\cdot\frac{x}{y}=\frac{ax}{by}\in\mathbb{Z}_{(2)}$

$\Rightarrow(\mathbb{Z}_{(2)},+,\cdot)$ subinel

Def: $(R,+,\cdot)$ un inel, $I\subseteq R$, I s.n. ideal la dr (resp st.) dacă

1) $\forall a,b\in I$, $a-b\in I$

2) $\forall a\in I$, $\forall r\in R$, $ar\in I\to$ ideal la dr ($r\cdot a\in I\to$ ideal la st)

obs: $I\subseteq R \Rightarrow \forall a,b\in I, a\cdot b\in I \Rightarrow I$ subinel

~~Def: I s.n~~

obs I s.n ideal bilateral dacă I ideal la st și dr.

ssae I ideal al lui $\mathbb{Z}_{(2)}$ $I=n\mathbb{Z}$, $n\in\mathbb{N}$

-Seminar-

Def: Fie $(R,+,\cdot)$ un inel și $I \subseteq R$, I s.n. ideal la st (sau dr) dacă
1) $\forall\, x,y \in I, x-y \in I$
2) $\forall\, r \in R, x \in I, rx \in I$ $(xr \in I)$

Ex: Idealele lui $(\mathbb{Z},+,\cdot)$ sunt $(\mathbb{Z}_n,+,\cdot)$

Ex: Det idealele inelului $(\mathbb{Z}_n,+,\cdot)$

Prop de universalitate a ~~grupului~~ inelului factor

$(R,+,\cdot)$, $(R',+,\cdot)$, $f: R \to R'$ un morfism surjectiv

$Ker f = \{x \in R \mid f(x) = 0_{R}\}$
↳ ~~nat~~ nucleul lui f

$\left.\begin{array}{l} I \trianglelefteq R \\ Ker f \subseteq I \end{array}\right\} \Leftrightarrow f(I) \trianglelefteq R'$

$\pi = f: \mathbb{Z} \to \mathbb{Z}_n$, $\pi(x) = \hat{x}$
↳ Proiecția canonică

$\tilde{\mathcal{I}}_{\mathbb{Z}_n} = \{f(I) \mid I \trianglelefteq \mathbb{Z}, Ker f \subseteq I\}$ ⇔ $k \mid n$

$I = k\mathbb{Z}$, $k \in \mathbb{N}$

$I \trianglelefteq \mathbb{Z}$, $\exists\, k \in \mathbb{N}$ a.î. $I = k\mathbb{Z}$

$Ker f = Ker \pi = n\mathbb{Z}$

$x \in Ker f \Rightarrow f(x) = \hat{0} \Rightarrow \hat{x} = \hat{0} \Leftrightarrow x = n\mathbb{Z}$

$Ker f = n\mathbb{Z} \subseteq k\mathbb{Z} \Leftrightarrow k \mid n$

$x \in n\mathbb{Z}$, $x = nt$, $t \in \mathbb{Z}$

$I_{\mathbb{Z}_n} = \{ \hat{k}\mathbb{Z}_n \mid k \mid n \}$

$(R,+,\cdot)$ un inel $I \trianglelefteq R$ a.î. $I = (a)$ (generat de un sg. element). A

I s.n ideal principal al lui R

K-corp comutativ, $K[X]$- are toate idealele principale

$I = (a) = \{ f \cdot a \mid f \in R \}$

Ex: $n\mathbb{Z} = (n) = \{nk \mid k \in \mathbb{Z}\}$

$I = (a_1, \dots, a_n) = \{ \sum_{i=1}^{n} f_i a_i \mid f_i \in R \}$

3. Arătăm că idealul $I = (\overset{f_1(x)}{2x^4 + 9x^3 + 13x^2 + 7x + 1}, \overset{f_2(x)}{2x^3 + 9x^2 + 11x + 4}) \trianglelefteq \mathbb{R}[X]$ este principal (găsiți $f \in \mathbb{R}[X]$ a.î. $I = (f)$)

$R[X]$

$f \in R[X]$ inversabil $\Leftrightarrow \begin{cases} a_0 \text{ este inversabil} \\ \text{și} \\ a_i \text{ nilpotent } \forall i > 0 \end{cases}$

$f = a_0 + a_1 X + \dots + a_n X$

$I = ((f_1, f_2))$

$\overset{\shortparallel}{f} = \text{cmmdc}(f_1, f_2)$

$\begin{cases} (R,+,\cdot) \text{ inel principal} \\ (a), (b) \\ (a)+(b) = (a,b) = ((a,b)) \end{cases}$

"$\subseteq$" $P \in I \Rightarrow \exists Q_1, Q_2 \in \mathbb{R}[X]$ a.î. $P = Q_1 f_1 + Q_2 f_2 \overset{?}{\Rightarrow} P \in (f)$

$f = (f_1, f_2) \Rightarrow \begin{cases} f \mid f_1 \Rightarrow f \mid Q_1 f_1 \\ f \mid f_2 \Rightarrow f \mid Q_2 f_2 \end{cases} \Rightarrow f \mid P \Rightarrow P \in (f) \Rightarrow I \subseteq (f)$

$P \in (f)$

$f \in I \Rightarrow (f) \subseteq I$

$f = (f_1, f_2) \underset{\substack{\uparrow \\ \text{Alg Euclid}}}{\Rightarrow} \exists\, P_1, P_2 \in \mathbb{R}[x]$ a.î. $P_1 f_1 + P_2 f_2 = f \Rightarrow$ ~~$f \in I$~~ $f \in (f_1, f_2) = I \Rightarrow$

$\Rightarrow f \in I \Rightarrow (f) \subseteq I$

.. Desc în polinoame ired polinomul

$$f = x^4 + 2x^3 + x^2 + 2x + 1 \in \mathbb{R}[x]$$

$t = x + \frac{1}{x}$

$t^2 = x^2 + \frac{1}{x^2} + 2$

$f = x^4 + 1 + 2x(x^2+1) + x^2 =$

$= x^2(x^2 + \frac{1}{x^2}) + 2x^2(x + \frac{1}{x}) + x^2 =$

$= x^2(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1)$

$\Rightarrow \frac{f}{x^2} = t^2 - 2 + 2t + 1$

$g(t) = t^2 + 2t - 1 = (t + 1 - \sqrt{2})(t + 1 + \sqrt{2})$

$\Delta = 4 + 4 = 8$

$t_{1,2} = \frac{-2 \pm 2\sqrt{2}}{2} \Leftrightarrow t_{1,2} = -1 \pm \sqrt{2}$

$\frac{f}{x^2} = (x + \frac{1}{x} + 1 - \sqrt{2})(x + \frac{1}{x} + 1 + \sqrt{2})$,

$f = x^2(x + \frac{1}{x} + 1 - \sqrt{2})(x + \frac{1}{x} + 1 + \sqrt{2})$

$f = [x^2 + 1 + (1 - \sqrt{2})x]\left(x + \frac{1+\sqrt{2} - \sqrt{2\sqrt{2}-1}}{2}\right)\left(x + \frac{1+\sqrt{2} + \sqrt{2\sqrt{2}-1}}{2}\right)$

5. Det morfismele de la $\mathbb{Z}_9$ la $\mathbb{Z}_{27}$

$$f: \mathbb{Z}_9 \to \mathbb{Z}_{27}$$

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

obs. $\mathbb{Z}_n = \langle \hat{1} \rangle$

$\hat{k} \in \mathbb{Z}_n$, $\hat{k} = \underbrace{\hat{1}+\dots+\hat{1}}_{\text{de } k \text{ ori}}$

$\hat{k} \in \mathbb{Z}_9$, $f(\hat{k}) = f(\underbrace{\hat{1}+\dots+\hat{1}}_{k \text{ ori}}) = f(\hat{1}) + \dots + f(\hat{1}) = k f(\hat{1})$

$$f(\hat{1}) = \bar{a}$$

$$f(\hat{k}) = \overline{ka}$$

$$\left.\begin{array}{l} f(\hat{0}) = \bar{0} \\ \parallel \\ f(\hat{9}) = \overline{9a} \end{array}\right\} \Rightarrow 9 \cdot \bar{a} = \bar{0} \Rightarrow 9a \in 27\mathbb{Z} \Rightarrow 27 \mid 9a$$

$$f(\hat{1}) = f(\hat{1}\cdot\hat{1}) = f(\hat{1}) \cdot f(\hat{1}) \Rightarrow \bar{a} = \bar{a}^2 \Rightarrow \bar{a} \in \mathrm{Idem}\,\mathbb{Z}_{27} = \{\bar{0}, \bar{1}\}$$

$$|\mathrm{Idem}\,\mathbb{Z}_{27}| = 2$$

$$27 = 3^3$$

Dacă $\bar{a} = \bar{0} \Rightarrow f(\hat{n}) = \bar{0}$.

Dacă $\bar{a} = \bar{1} \Rightarrow f(\hat{n}) = \bar{n}$, dar $27 \nmid 9$ Fals

---

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "f"'] & G/H \\ G' & \end{tikzcd}$$

~~Dacă ∄~~

Dacă $\mathrm{Ker} f \supseteq H \Rightarrow \exists!\ f'$ morfism de la G/H la G'

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}_m \arrow[dl, "\exists!"] \\ \mathbb{Z}_n & \end{tikzcd}$$

16.04.2018

Algebră

- Seminar -

Th fundam de izomorfism (TFI)

<u>TFI</u>: $(R_1,+,\cdot)$, $(R_2,+,\cdot)$ 2 inele și $f: R_1 \to R_2$ morfism de inele

$\operatorname{Ker} f = \{x \in R_1 \mid f(x) = 0\}$

$\operatorname{Im} f = \{y \in R_2 \mid \exists x \in R_1 \text{ a.î. } f(x) = y\}$

Atunci $\exists!\ \bar{f}: \frac{R_1}{\operatorname{Ker} f} \to \operatorname{Im} f$, $\bar{f}(\hat{x}) = f(x)$

$\bar{f}(\pi(x)) = f(x)$

$\bar{f} \circ \pi = f$

Ex 1: Să se $\frac{\mathbb{Q}[X]}{(X-1)} \simeq \mathbb{Q}$

$f: \mathbb{Q}[X] \to \mathbb{Q}$; $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$

$f(P) = P(1)$

$P_1, P_2 \in \mathbb{Q}[X]$, $f(P_1+P_2) = (P_1+P_2)(1) = P_1(1) + P_2(1) = f(P_1) + f(P_2)$

$f(P_1 \cdot P_2) = (P_1P_2)(1) = P_1(1)P_2(1) = f(P_1)f(P_2)$

$a \in \mathbb{Q}$; $P = a$, $f(P) = a \Rightarrow f$ surj.

$\operatorname{Ker} f = \{P \in \mathbb{Q}[X] \mid f(P) = 0\} = \{P \in \mathbb{Q}[X] \mid P(1) = 0\} \overset{\text{Th. Bézout}}{=} \{P \in \mathbb{Q}[X] \mid X-1 / P\} \subseteq (X-1)$

$\cancel{f((X-1))}$ $\quad (X-1) \subseteq \operatorname{Ker} f$ $\quad \Big\} \Rightarrow$

$\Rightarrow \operatorname{Ker} f = (X-1) \overset{TFI}{\Rightarrow} \frac{\mathbb{Q}[X]}{(X-1)} \simeq \mathbb{Q}$

2. Sa se $\frac{\mathbb{Z}[x]}{(x^2+1)} \simeq \mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$

$f: \mathbb{Z}[x] \to \mathbb{Z}[i]$

~~f morfism surj ($\mathrm{Im} f = \mathbb{Z}[i]$)~~

$\mathrm{Ker} f = (x^2+1)$

Alegem $f(P) = P(i)$

$f(P+Q) = (P+Q)(i) = P(i)+Q(i) = f(P)+f(Q)$

$f(P \cdot Q) = (PQ)(i) = P(i) \cdot Q(i) = f(P) \cdot f(Q)$ $\Big\} \Rightarrow f$ morfism

Fie $a+bi \in \mathbb{Z}[i]$

Alegem $P = bx + a$

$f(P) = P(i) = \cancel{b} \; b \cdot i + a = a + bi \Rightarrow \exists P \in \mathbb{Z}[x]$ a.î. $f(P) = a+bi$;

$\forall a,b \in \mathbb{Z} \Rightarrow f$ surj $\Rightarrow \mathrm{Im} f = \mathbb{Z}[i]$

$f(P) = 0 \Leftrightarrow P(i) = 0 \Leftrightarrow (x-i) \mid P \Rightarrow x-i \mid P$

$x+i \mid P \quad (\Rightarrow) \quad (x-i)(x+i) \mid P \Leftrightarrow$

$\Leftrightarrow (x^2+1) \mid P \Leftrightarrow P = (x^2+1) Q \Leftrightarrow P \in (x^2+1)$

3. Sa se $\frac{\mathbb{Z}[x]}{(x^2-1)} \simeq A = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \in 2\mathbb{Z}\}$

$f: \mathbb{Z}[x] \to A$

$f(P) = (P(1), P(-1)) \overset{?}{\in} A$

$P = a_0 + a_1 x + \dots + a_n x^n$

$P(1) = a_0 + a_1 + \dots + a_n$

$P(-1) = a_0 + a_1 + \dots + (-1)^n a_n$

$P(1) + P(-1) = 2a_0 + 0 \cdot a_1 + 2 \cdot a_2 + 0 \cdot a_3 + \dots + \begin{cases} 2a_n, & n = 2k \\ 0 \, a_n, & n = 2k+1 \end{cases}$

Fie $P_1, P_2 \in \mathbb{Z}[x]$

$f(P_1 + P_2) = ((P_1+P_2)(1), (P_1+P_2)(-1)) = (P_1(1)+P_2(1), P_1(-1)+P_2(-1)) =$

$= (P_1(1), P_1(-1)) + (P_2(1), P_2(-1)) = f(P_1) + f(P_2)$

Analog $f(P_1 \cdot P_2) = f(P_1) f(P_2) \Rightarrow f$ este morfism $\Big\} \Rightarrow f$ morfism

Fie $(a,b) \in A \Leftrightarrow a-b \in 2\mathbb{Z}$

$f(P) = (a,b)$

$(P(1), P(-1)) = (a,b)$

$P(1) = a$

$P(-1) = b$

$P(x) = \frac{a+b}{2} + \frac{(a-b)x}{2} \in \mathbb{Z}[x] \Rightarrow f$ surj

~~$\ker f = (x^2-1)$~~

Fie $P \in \ker f \Rightarrow \left.\begin{array}{l} P(1) = 0 \Rightarrow (x-1) \mid P \\ P(-1) = 0 \Rightarrow (x+1) \mid P \end{array}\right\} \Leftrightarrow (x^2-1) \mid P \Rightarrow \exists Q$ a.î. $P = (x^2-1)Q$

$\Rightarrow P \in (x^2-1) \Rightarrow \ker f \subseteq (x^2-1)$

Fie $P \in (x^2-1) \Rightarrow P = Q(x-1)(x+1) \Rightarrow \left.\begin{array}{l} P(1) = Q \cdot 0 \cdot 2 = 0 \\ P(-1) = 0 \end{array}\right\} \Rightarrow P \in \ker f \Rightarrow (x^2-1) \subseteq \ker f$

$\Rightarrow \ker f = (x^2-1)$

$\xRightarrow{TFI} \frac{\mathbb{Z}[x]}{(x^2-1)} \simeq A$

07.05.2018

Algebră

– Seminar –

Polinoame simetrice

Fie R un inel comutativ și unitar.

$R[x_1, x_2, \dots x_n] = \{ f = \sum_{\text{finită}} c \cdot x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n},\ c \in R,\ \alpha_i \in \mathbb{N},\ i = \overline{1,n} \}$

$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots x_n^{\alpha_n}$ s.n. monom.

$a = x_1^{\alpha_1} \dots x_n^{\alpha_n}$

$b = x_1^{\beta_1} \dots x_n^{\beta_n}$

ordinea lexicografică pe mulțimea monoamelor:

$a < b \Leftrightarrow (\text{grad}(a) < \text{grad}(b))$ sau $(\text{grad}\, a = \text{grad}\, b$ și $\exists k = \overline{0, n-1}$ a.î.

$\alpha_i = \beta_i, \forall i = \overline{1,k}$ și $\alpha_{k+1} < \beta_{k+1})$

$\text{grad}\, a = \sum_{i=1}^{n} \alpha_i$ $\quad (x_1 x_2^2 > x_3^3)$

$\alpha = (\alpha_1, \dots \alpha_n)$

$\beta = (\beta_1 \dots \beta_n)$ $\quad \alpha - \beta = (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$

vectorul $\alpha - \beta$ are prima comp nenulă din stânga negativă

Ex 1: Toate monoamele de grad 3 din $\mathbb{C}[x_1, x_2, x_3]$ în ordine desc

$x_1^3 > x_1^2 x_2 > x_1^2 x_3 > x_1 x_2^2 > x_1 x_2 x_3 > x_1 x_3^2 > x_2^3 > x_2^2 x_3 > x_2 x_3^2 > x_3^3$

$f \in R[x_1, \dots x_n]$, $\sigma \in S_n$ def morfismul de inele

$\bar{\sigma} : R[x_1, \dots x_n] \to R[x_1 \dots x_n]$

$f = \sum c\, x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

$\bar{\sigma}(f) = \sum c\, x_{\sigma(1)}^{\alpha_1} x_{\sigma(2)}^{\alpha_2} \dots x_{\sigma(n)}^{\alpha_n}$

Def: Un polinom $f \in R[x_1, \dots x_n]$ s.n simetric dacă σ ... Pasul ...

$f = x_1^\alpha + x_2^\alpha + x_1x_2$

Th fundam a pol simetrice

Considerăm
$S_1 = x_1 + \dots + x_n$
$S_2 = x_1x_2 + x_1x_3 + \dots x_{n-1}x_n$
$S_3 = x_1x_2x_3 + \dots + x_{n-2}x_{n-1}x_n$
$\dots$
$S_n = x_1x_2 \dots x_n$

Polinoamele simetrice fundam

Al. orice polinom simetric $f \in R[x_1, \dots x_n]$ se scrie ca polinom ~~de~~ de polinoame simetrice

$f = x_1^2 + x_2^2 + x_1x_2 = f(x_1, x_2) \in C[x_1, x_2]$

$S_1 = x_1 + x_2$
$S_2 = x_1x_2$
$f(S_1, S_2) = S_1^2 - S_2$

Ex: $f = x_1^3x_2 + x_1^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2^3x_3 + x_2x_3^3$

Det scrierea lui f ca polinom de polinoame simetrice

Pasul 1: Det cel mai mare monom din scrierea lui $f = x_1^3x$

Pasul 2: Scriem în ordine descresc. toate monoamele de grad = grad$(x_1^3x_2) = 4$ din $C[x_1, x_2, x_3]$ mai mici decât $x_1^3x_2$

$x_1^3x_2 > x_1^3x_3 > x_1^2x_2x_3 > x_1^2x_3^2 > x_1x_2^3 > x_1x_2^2x_3 > x_1x_2x_3^2 > x_1x_3^3 >$
$> x_2^4 > x_2^3x_3 > x_2^2x_3^2 > x_2x_3^3 > x_3^4$

Pasul 3:

$a = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$, $\alpha = (\alpha_1, \alpha_2, \alpha_3)$

Din șirul obținut la pasul 2, păstrăm doar monoamele de forma $a = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$ și $\alpha_1 \geq \alpha_2 \geq \alpha_3$

$x_1^3 x_2 > x_1^2 x_2^2 > x_1^2 x_2 x_3$

Pasul 4: $f(s_1, s_2, s_3) = s_1^{3-1} s_2^{1-0} s_3^{0} + a s_1^{2-2} s_2^{2-0} s_3^{0} + b s_1^{2-1} s_2^{1-1} s_3^{1}$

$(3,1,0)$ $(2,2,0)$ $(2,1,1)$

$f((1,0,1)) = 2$

$s_1 = x_1 + x_2 + x_3 = 2$

$s_2 = x_1x_2 + x_1x_3 + x_2x_3 = 1$

$s_3 = x_1x_2x_3 = 0$

$2 = f(s_1, s_2, s_3) = 4 + a \Rightarrow a = -2$

3. $f = (x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2) \in \mathbb{C}[x_1, x_2, x_3]$

Pasul 1: Monomul maxim este $x_1^4 x_2^2$

Pasul 2: $x_1^4 x_2^2 > x_1^4 x_2 x_3 > \cancel{x_1^4 x_3^2} > x_1^3 x_2^3 > x_1^3 x_2^2 x_3 > x_1^2 x_2^2 x_3^2$

Pasul 3: $(4,2,0)$ $(4,1,1)$ $(3,3,0)$ $(3,2,1)$ $(2,2,2)$

Pasul 4: $f(s_1, s_2, s_3) = s_1^{4-2} s_2^2 + a \cdot s_1^3 s_3 + b s_2^3 + c s_1 s_2 s_3 + d s_3^2$

Pasul 5: $f((0,1,1)) = 2 = 4 + b \Rightarrow b = -2$

$f((0,0,1)) = 0$

$f((-1,0,1)) = 8 = 81 + a \cdot 27 - 18 + 9c + d$

$f((-1,-1,2)) = 50 = 54 + 4d \Rightarrow d = -1$

$s_1 = x_1 + x_2 + x_3 = 1$

$s_2 = x_1x_2 + x_1x_3 + x_2x_3 = 0$

$s_3 = x_1x_2x_3 = 0$

$b = -2$

$27a + 9c = 18$

$d = -1$

$f((2,2,-1)) = 200 = 0 - 108a - 16 \Rightarrow -108a = \cancel{216} \; 216 \Rightarrow a = -2$

14.05.2018

Algebră

-Seminar-

Sistem de ec. liniare

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{n1}x_1 + \dots + a_{nn}x_n = b_n \end{cases}$$

1. Metoda Cramer.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \qquad b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$\det A \neq 0 \iff$ sist (1) are o unică sol $x_i = \frac{\Delta_i}{\det A}$; Δ_i det matricei obținute prin înloc. coloanei i cu b

$\det A = 0$

$A^e = (A, b)$ sist este comp $\iff \text{rang} A = \text{rang} A^e$

2. Dacă $\det A \neq 0$, $\exists A^{-1}$ și $x = A^{-1}b$

3. Def. 2 sisteme s.n echivalente dacă au ac. nr de sol și toate sol sunt egale sau ambele sunt incomp.

2. Gauss

Transform elem.

1. Permutarea a 2 linii
2. Înmulțirea unei ec cu un scalar
3. Adun unei ec cu alta

Ex 1:

$$\begin{cases} 8x_1 - x_2 - x_3 + x_4 = -1 \\ x_1 + x_2 + x_3 + x_4 = 5 \\ 5x_1 + 3x_2 - 6x_3 + 2x_4 = -7 \\ 3x_1 + 2x_2 - 3x_3 + x_4 = 2. \end{cases}$$

[Insert Gauss here]

2. $$\begin{cases} 2x_1 - x_2 - x_3 = -1 \\ 3x_1 + 3x_2 + 2x_3 = -1 \\ 8x_1 + 5x_2 + 3x_3 = 2 \end{cases}$$

[Analog]