Algebră II
Curs 1 (nou)

① Inele și Corpuri

Inele

Def: R mulțime și +, ∘ sunt două operații pe R

R mulțime —> Operație

* operație pe R, e o funcție de la $R \times R$ cu valori în R

(R, +, ∘) s.n. inel dacă:

1) (R, +) grup comutativ

2) ∘ asociativă și există element neutru pt „∘"

3) $x \cdot (y+z) = x \cdot y + x \cdot z, \ \forall x, y, z \in \mathbb{R}$
$(x+y) \cdot z = x \cdot z + y \cdot z, \ \forall x, y, z \in \mathbb{R}$ } distributivitatea înmulțirii față de adunare

+, ∘ —> 2 operații oarecare, nu obligator adunare și înmulțire clasică.

Convenție: Elementul neutru față de + se notează cu 0
Elementul neutru față de ∘ se notează cu 1

Reguli de calcul: $x \cdot 0 = 0$

$$x \cdot 0 = x \cdot (0+0) \overset{3}{=} x \cdot 0 + x \cdot 0$$

$$y + 0 = y$$

$x \cdot 0$ are invers în grupul $(R, +)$

notăm cu z inversul $z + x \cdot 0 = 0$.

$$\underbrace{z + x \cdot 0}_{0} = z + (x \cdot 0 + x \cdot 0) \overset{2}{=} \underbrace{(z + x \cdot 0)}_{0} + x \cdot 0$$

$$= x \cdot 0 \Rightarrow x \cdot 0 = 0$$

Convenție:

Notăm inversul lui x în $(R, +)$ grup cu $-x$

Reguli de calcul

$$x \cdot (-y) = (-x) \cdot y = -xy$$

Dem

$$0 = x \cdot 0 = x \cdot (y - y) \overset{3}{=} x \cdot y + x \cdot (-y) \quad | + -x \cdot y$$

$$-xy + 0 = -\underbrace{xy + xy}_{0} + x \cdot (-y)$$

$$-xy = x \cdot (-y)$$

$$(-x) \cdot (-y) = xy$$

Dem

$$\underset{\overset{\shortparallel}{0}}{0} = (x - x) \cdot (-y) \overset{4}{=} x \cdot (-y) + (-x) \cdot (-y)$$

$$0 = -xy + (-x) \cdot (-y) \quad | + xy$$

$$0 + xy = -\underbrace{xy + xy}_{0} + (-x) \cdot (-y)$$

R vine de la cuvântul englez Ring

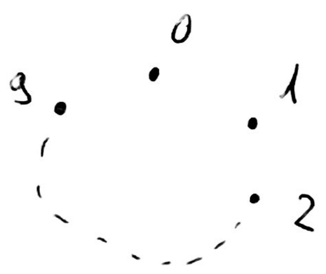
$$xy = (-x) \cdot (-y)$$

Exemple $(\mathbb{R}, +, \cdot)$ $(\mathbb{Q}, +, \cdot)$
↳ nr reale

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

$n \in \mathbb{N}$, $n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$
↳ mulțimea claselor de resturi modulo n.

$\mathbb{Z}_{10}$



$\bar{0} = \overline{10} = \overline{20} = \overline{30}$ => înfășor mulțimea nr întregi pe cerc => de aici vine denumirea ring (R = inel)

Elemente inversabile în inel

$u \in R$ s.n. inversabil dc $\exists\, v \in R$ cu $u \cdot v = v \cdot u = 1$

$U(R) = \{u \in R \mid u \text{ inversabil}\}$
↳ „unit" sau
$\{u \in R \mid \exists\, v \in R \text{ cu } u \cdot v = v \cdot u = 1\}$

Def. $(K, +, \cdot)$ corp $\iff \begin{cases} (K, +, \cdot) \text{ inel} \\ \text{și } U(K) = K \setminus \{0\} \end{cases}$
↳ elem neutru față de I op

Dem $(R,+,\cdot) \rightarrow$ corp

$(\mathbb{Z},+,\cdot) \rightarrow$ nu e corp
e doar inel

$(\mathbb{Q},+,\cdot) \rightarrow$ corp

$(\mathbb{C},+,\cdot) \rightarrow$ corp

$U(\mathbb{Z}) = \{+1,-1\} \Rightarrow \pm\, \mathbb{Z}\setminus\{0\} \Rightarrow (\mathbb{Z},+,\cdot)$ nu e corp

Exp: Inele de — polinoame
— matrici

Exp: Criptare cu matrici

Inel comutativ $(R,+,\cdot)$

Def: $(R,+,\cdot)$ s.n. comutativ dacă cea de-a 2-a operație este comutativă $a\cdot b = b\cdot a,\ \forall\, a,b\in R$

$n \in \mathbb{N},\ n \geq 2$

Inelul de matrici (tablouri $n\times n$)

$$\mathcal{M}_n(R) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \;\middle|\; \begin{array}{l} a_{ij}\in R \\ \forall\, i,j=\overline{1,n} \end{array} \right\}$$

scriere condensată

$A = (a_{ij})_{1\leq i,j\leq n}$

$B = (b_{ij})_{1\leq i,j\leq n}$

Def

$A+B=C=(c_{ij})_{1\le i,j\le n}$ $\quad c_{ij}=a_{ij}+b_{ij}$

$A\cdot B=D=(d_{ij})_{1\le i,j\le n}$

$$d_{ij}=\sum_{k=1}^{n} a_{ik}\cdot b_{kj}$$

$(\mathcal{M}_n(R),+,\cdot)$ = inel de matrici $n\times n$ cu coeficienți în inelul R

Elem neutru pt + este $\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = O_n$

Elem neutru pt $\cdot$ este $\begin{pmatrix} 1 & \cdots & & 0 \\ \vdots & 1 & & \vdots \\ \vdots & & 1 & 1 \\ 0 & \cdots & & \end{pmatrix} = I_n$

Criptare cu matrici

Alfabet

0	1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M	H

14	15	16	17	18	19	20	21	22	23	24	25
O	P	Q	R	S	T	U	V	W	X	Y	Z

$A\in U(\mathcal{M}_n(\mathbb{Z}_{26}))$ → matrice inversabilă cu coeficienți în $\mathbb{Z}_k$

R inel $\quad$ $\mathbb{Z}_k$ → k = lungime alfabet

$U(R) = \{r \in R \mid \exists\, s \in R$ cu $r \cdot s = s \cdot r = 1\}$

o secvență de n simboluri se transformă într-o secvență de n simboluri după următoarea regulă:

secv $(x_1, x_2, \dots x_n) \longrightarrow (y_1, y_2, \dots y_n)$

$A = (a_{ij})_{1 \le i,j \le n}$

după următoarea regulă:

$$y_j = \sum_{k=1} a_{jk} x_k \quad \forall j = \overline{1,n}$$

Exemplu

$A = \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{7} & \bar{4} \end{pmatrix} \in U(M_2(\mathbb{Z}_{26}))$ → matricea de criptare

→ trebuie să fie inversabilă

$n = 2$

Mesaj: ST|OP|TR|AH|SP|OR|TX → $\overline{18}\ \overline{19}\quad \overline{14}\ \overline{15} \dots$

→ $\bar{3}\ \overline{20}\quad \overline{17}\ \bar{2} \dots$

→ D U RC ...

$$A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

ST → 18, 19

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{7} & \bar{4} \end{pmatrix} \begin{pmatrix} \overline{18} & \overline{14} \\ \overline{19} & \overline{15} \end{pmatrix} = \begin{pmatrix} \bar{3} & \overline{17} \\ \overline{20} & \bar{2} \end{pmatrix}$$

$$D = A \cdot B = d_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

$\overline{2 \cdot 18} + \overline{1 \cdot 19}$

$= \overline{36 + 19} = \overline{10 + 1\ldots}$

$= \overline{29} = \bar{3}$

$\overline{2 \cdot 14} + \overline{1 \cdot 15} = \overline{28} + \overline{15} = \bar{2} + \overline{15} = \overline{17}$

$\overline{7 \cdot 18} + \overline{4 \cdot 19} = \overline{126} + \overline{76} = \overline{202} = \overline{20}$

$\overline{7 \cdot 14} + \overline{4 \cdot 15} = \overline{98} + \overline{60} = \overline{158} = \bar{2}$

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{7} & \bar{4} \end{pmatrix} \begin{pmatrix} \bar{4} & -\bar{1} \\ -\bar{7} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

$$\begin{pmatrix} \bar{4} & -\bar{1} \\ -\bar{7} & \bar{2} \end{pmatrix} \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{7} & \bar{4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

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

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

$\bar{r} \in U(\mathbb{Z}_n) \Rightarrow \exists\, \bar{s}$ a.î. $\bar{r} \cdot \bar{s} = \bar{1}$

$\bar{s} \cdot \bar{r} = \bar{1}$

$|U(\mathbb{Z}_n)| = \varphi(n) =$

$= n \cdot \prod \left(1 - \frac{1}{p}\right)$

p prim

$p \mid n$

Inversul lui $\bar{3}$ în $(\mathbb{Z}_{26}, +, \cdot)$

I metodă

$\overline{3} \cdot \overline{x} = \overline{1}$

$\overline{3} \cdot \overline{9} = \overline{27} = \overline{1}$

$\overline{31} \cdot \overline{x} = \overline{1} \quad \mathbb{Z}_{101}$

$-\overline{8} \cdot \overline{x} = \overline{93} \cdot \overline{x} = \overline{3}$

$\overline{31} \cdot \overline{3} = \overline{93}$

$\overline{31} \cdot \overline{4} = \overline{124}$

$\overline{8} \cdot \overline{x} = -\overline{3} = \overline{98}$

$\overline{4x} = \overline{49} = \overline{49+101} = \overline{150}$

$\overline{2x} = \overline{75} = \overline{75+101} = \overline{176}$

$\Rightarrow x = \overline{88}$

metodo II. Alg lui Euclid

$101 = 31 \cdot \boxed{3} + 8$

$31 = 8 \cdot \boxed{3} + 7$

$8 = 7 \cdot \boxed{1} + 1$

$7 = 7 \cdot \boxed{1}$

$3 + \cfrac{1}{3 + \cfrac{1}{1}} = 3 + \frac{1}{4} = \frac{13}{4}$

$\frac{101}{31} - \frac{13}{4} = \frac{-(1)^{n \text{ op alg}}}{31 \cdot 4} = \frac{1}{31 \cdot 4}$

$4 \cdot 101 - 31 \cdot 13 = 1$

$404 - 403 = 1$

$\overline{-13} = \overline{88}$

$31 \cdot (-13) \equiv 1 (\text{mod } 101)$

$(\mathbb{Z}_n, +, \cdot) \quad n \geq 2$

– Când este corp?

$|U(\mathbb{Z}_n)| = \varphi(n)$

$\mathbb{Z}_n$ corp $\Leftrightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{\overline{0}\}$

$\Leftrightarrow |U(\mathbb{Z}_n)| = |\mathbb{Z}_n \setminus \{\overline{0}\}| = n-1 \Leftrightarrow$

$\Leftrightarrow \varphi(n) = n-1 \Leftrightarrow n = \text{prim}$

$\varphi(n) = n \cdot \prod \left(1 - \frac{1}{p}\right) = \left|\{m \in \mathbb{N} \mid 0 \leq m \leq n-1, (m,n)=1\}\right|$

p prim
$p \mid n$

$$\varphi(n) = n-1 \Leftrightarrow \begin{cases} (m,n) = 1 \\ \forall m \in \{1, 2, \dots n-1\} \end{cases}$$

Teoremă: $\mathbb{Z}_n$ corp $\Leftrightarrow n$ prim

Exemplu:

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ $\quad U(\mathbb{Z}[i]) = ? = \{\pm 1, \pm i\}$

$(\mathbb{Z}[i], +, \cdot)$ - inel

adunare și înmulțire de numere complexe

$(a+bi) + (c+di) = a + c + (b+d)i$

$(a+bi)(c+di) = ac - bd + i(ad + bc)$

În acest inel avem element inversabil $1 \cdot 1 = 1$

$i^2 = -1$

$i \cdot (-i) = 1$

$(a+bi)(c+di) = 1$ $\quad$ vom arăta că nu mai există alte elemente neutre

$a + bi \in \{\pm 1, \pm i\}$

x, d)

$$\begin{aligned} ac - bd &= 1 \quad \Big| \cdot c \\ ad + bc &= 0 \quad \Big| \cdot d \end{aligned} \quad (+)$$

$$a(c^2+d^2) = c \qquad a = \frac{c}{c^2+d^2} \in \mathbb{Z}$$

$$\frac{|c|}{c^2+d^2} \in \mathbb{N} \qquad |c| = (c^2+d^2) \cdot k$$

$$k \in \mathbb{N}$$

$$k = 0 \Rightarrow c = 0 \Rightarrow \left.\begin{aligned} bd &= -1 \\ ad &= 0 \\ d &\neq 0 \end{aligned}\right| \Rightarrow \begin{aligned} a &= 0 \\ d &= \pm 1 \end{aligned}$$

$$\Rightarrow c + di = \pm i$$

$$|c| = (c^2+d^2) \cdot k$$

$$|c| \geq c^2 + d^2 \geq c^2 \Rightarrow c = 0, \pm 1$$

$c = \pm 1$

$$1 = (1+d^2) \cdot k \Rightarrow d = 0$$

$$c + di = \pm i, \pm 1$$

Exp: $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

$U(\mathbb{Z}[\sqrt{2}]) = ?$

↓ mulțime infinită

$(\mathbb{Z}[\sqrt{2}], +, \cdot)$

↘ adunare și înmulțire de nr reale

$(R,+,\cdot)$ inel $\Rightarrow \pm 1 \in U(R)$ $\qquad \bar{1} = -\bar{1}$ $\mathbb{Z}_2$

$(-1)(-1) = 1$ $\qquad$ Inel când

$(a+b\sqrt{2})(c+d\sqrt{2}) = 1$

$a,b,c,d \in \mathbb{Z}$

$\sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$ $\qquad \sqrt{2}(a+b\sqrt{2}) = 1$

$2b + a\sqrt{2} = 1$

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

$\sqrt{2} = 1 - \frac{2b}{a} \in \mathbb{Q}$

$u \in U(R) \Rightarrow u^n \in U(R)$

$\sqrt{2} \notin \mathbb{Q} \Rightarrow a = 0$

$U(\mathbb{Z}[\sqrt{2}]) = \{\pm(\sqrt{2}+1)^n \mid n \in \mathbb{Z}\}$

$2b = 1$

$b = 1/2 \notin \mathbb{Z}$

Algebră II C1 (non) test

1. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Matrice de criptare $\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{5} & \bar{4} \end{pmatrix}$. Am interceptat mesajul UP. Decriptați

$\in (\mathcal{M}_2(\mathbb{Z}_{26}))$

2. Găsiți matricea inversă $\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{5} & \bar{4} \end{pmatrix}$ din $\mathcal{M}_2(\mathbb{Z}_{26})$

$$\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{5} & \bar{4} \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{5} & \bar{4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$$

3. $\mathbb{Z}[\sqrt{14}] = \{a + b\sqrt{14} \mid a, b \in \mathbb{Z}\}$

Găsiți un exemplu $u \in U(\mathbb{Z}[\sqrt{14}])$ $u \neq \pm 1$

$(\mathbb{Z}[\sqrt{14}], +, \cdot)$

adunarea și înmulțirea din $\mathbb{R}$

4. Găsiți inversul lui $\overline{61}$ în $(\mathbb{Z}_{103}, +, \cdot)$ $\overline{61} \cdot \overline{x} = \overline{1}$

5. Găsiți soluțiile ec:

$$x^2 = x \text{ în } (\mathbb{Z}_{72}, +, \cdot)$$

Rezolvare Test

1. $\bar{2}x + \bar{y} = \overline{20} \quad | \cdot \bar{4}$ $\qquad y = \overline{20}$

$5x + \overline{4y} = \overline{15}$ $\qquad \Rightarrow$ mesaj = HU

$\overline{8x} + \overline{4y} = \overline{80} = \bar{2}$

$\overline{5x} + \overline{4y} = \overline{15}$

$\overline{3x} = -\overline{13} = \overline{13} \quad | \cdot \bar{9}$

$\bar{x} = \overline{13} \cdot \bar{9} = \overline{13} \cdot \bar{8} + \overline{13} = \overline{13} = x$

2. $\bar{2}a + c = \bar{1}$ $\qquad \bar{2}a + \bar{c} = \bar{1} \quad | (-4)$

$\bar{2}b + d = \bar{0}$ $\qquad 5a + 4c = \bar{0}$

$5\bar{a} + \bar{4}\bar{c} = \bar{0}$ $\qquad -\overline{3a} = -4$

$\bar{5}b + \bar{4}\bar{d} = \bar{1}$ $\qquad \overline{3a} = \bar{4} \quad | \cdot \bar{9}$

$\qquad a = \overline{36} = \overline{10}$

$c = \overline{1 - 2a}$

$= \overline{1 - 20} = -\overline{19} = \bar{7}$

$c = 7$ $\qquad \bar{2}\bar{b} + \bar{d} = \bar{0} \quad | \cdot (-4)$

$\qquad \bar{5}\bar{b} + \bar{4}\bar{d} = \bar{1}$

$-\overline{3b} = 1 \quad | \bar{9}$ $\qquad d = \overline{2b} = (\overline{-2}) \cdot (-\bar{9}) = -\overline{18}$

$-\bar{b} = \bar{9}$ $\qquad d = \overline{18}$

$b = \overline{17}$

metode 2.

$\det = 2\cdot4-5\cdot1=3$ $\qquad \frac{1}{3}\begin{pmatrix}4 & -1\\ -5 & 2\end{pmatrix}$ inversa în $\mathbb{Q}$

Inversul lui $\bar{3}$ este $\bar{9}$ $\qquad \bar{3}\cdot\bar{9}=\bar{1}$

$= \bar{9}\begin{pmatrix}\bar{4} & -\bar{1}\\ \overline{-5} & 2\end{pmatrix} = \begin{pmatrix}\overline{36} & -\bar{9}\\ \overline{-45} & \overline{18}\end{pmatrix}$

3. $(a+b\sqrt{14})(a-b\sqrt{14})=1$ $\qquad (a+b)(a-b)=a^2-b^2$

$a^2-14b^2=1$

$a^2-14\cdot4^2=1$ $\qquad 14\cdot16=(15-1)(15+1)=15^2-1$

$15^2-14\cdot16=15^2-(15^2-1)=1$

$15+4\sqrt{14}\in U(\mathbb{Z}[\sqrt{14}])$

4. $\overline{61}\cdot\bar{x}=\bar{1}$ $\quad \mathbb{Z}_{103}$

$103=61\cdot1+42$

$61=42\cdot1+19$

$42=19\cdot2+4$

$19=4\cdot4+3$

$4=3\cdot1+1$

$3=1\cdot3$

$1+\cfrac{1}{1+\cfrac{1}{2+\frac{1}{4}+\frac{1}{1}}} = 1+\cfrac{1}{1+\frac{5}{11}}$

$= 1+\frac{11}{16}=\frac{27}{16}$

$\frac{103}{61} = \frac{27}{16} = \frac{(-1)^6}{61\cdot16} =$

$103\cdot16-61\cdot27=1$ verificăm

$61\cdot(-27)\equiv1\ (103)$

$x=\overline{-27}=\overline{76}$

$\begin{array}{r}103\cdot\\16\\\hline 618\\103\ \ \\\hline 1648\end{array}$ $\quad 1648 \quad$ $\begin{array}{r}27\cdot\\61\\\hline 27\\162\ \ \\\hline 1647\end{array}$

metoda 2

$\overline{61}\cdot\overline{x}=\overline{1} \quad \mid \cdot\overline{2}$

$\overline{122}\cdot\overline{x}=\overline{2}$

$\overline{19}\cdot\overline{x}=\overline{2} \quad \mid \cdot\overline{5}$

$\overline{95}\cdot\overline{x}=\overline{10}$

$4\overline{x}=-\overline{5}=-\overline{108}$

$x=-\overline{27}=\overline{76}$

5. $\mathbb{Z}_{72}$ $\quad x^2=x$

$8\cdot 9=72 \mid x(x-1)$

$(x, x-1) \leftarrow$ prime între ele

$\overline{I}$ $72\mid x \qquad x=\overline{0}$

$\overline{II}$ $72\mid x-1 \qquad x=\overline{1}$

$\overline{III}$ $8\mid x \qquad 9\mid x-1$

$\overline{IV}$ $8\mid x-1 \qquad 9\mid x$

$\overline{IV}$ $x=9t=1+8s \qquad t=8u+1$

$9t\overset{8}{\equiv}1 \qquad x=9t=9(8u+1)=$

$t\overset{8}{\equiv}1 \qquad \overline{x}=\overline{9} \qquad 72u+9$

$\overline{III}$ $x=8t$

$0\overset{8}{\equiv}x-1=9s\overset{8}{\equiv}1+s \qquad s\equiv 7\ (8)$

- -

$s = 8u + 7$

$x = 1 + 9s = 1 + 9(8u + 7) = 72u + 64$

$\overline{x} = \overline{64}$

Soluții : $\overline{0}, \overline{1}, \overline{9}, \overline{64}$

$(R, +, \cdot)$ inel

r - idempotent dacă $r^2 = r$