18.12.2021

Tutoriat 9

Inele () și ce mai apucăm

Inelele în matematică 

Inel $\overset{def}{=}$ un triplet (R, α, β), unde R = o mulțime nevidă; $\alpha, \beta : R \times R \to R$ a. î.

1) (R, α) grup abelian; notăm $\alpha((a,b)) \overset{not}{=} a+b, \ \forall a,b \in R$
elementul neutru $= 0_R$ sau 0

2) (R, β) monoid; notăm $\beta((a,b)) \overset{not}{=} a \cdot b, \ \forall a,b \in R$
elem. neutru $= 1_R$ sau 1

3) Distributivitatea
- $a(b+c) = ab + ac$
- $(a+b)c = ac + bc$

$\forall a, b, c \in R$

În plus, $(R, +, \cdot)$ este inel comutativ dacă $ab = ba, \ \forall a, b$.

Ex inele: 1) cel mai faimos inel: $(\underbrace{\mathbb{N}, +}_{grup?}, \cdot)$ NU MERGE

Dar $(\mathbb{Z}, +, \cdot)$ MERGE

2) Ce inele au $0 = 1$?
Răspunsul: $\{0\}$ (inelul nul) $(\{0\}, +, \cdot)$

3) inele care (vom nota că) sunt mai mult decât inele:
$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

4) „Inelul întregilor lui Gauss"
$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

5) $(M_n(R), +, \cdot)$, unde R = inel
inelul matricelor de ordin n cu elemente din R

$0_{M_n(R)} = O_n$ (matricea cu elem. nule)

$1 = I_n \left(\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \right)$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Obs: pt. $n \geq 2$, $M_n(R)$ e necomutativ.

Def: R inel, $a \in R$

1) a s.n. DIVIZOR AL LUI ZERO LA STÂNGA (respectiv LA DREAPTA) dacă $\exists b \neq 0$ a.î. $ab = 0$ (respectiv $ba = 0$)

a s.n. DIVIZOR AL LUI ZERO dacă e divizor al lui zero și la stânga, și la dreapta.

* R s.n. INTEGRU dacă 0_R este singurul divizor al lui zero
* Un inel comutativ și integru s.n. DOMENIU DE INTEGRITATE.

Ex: . Domenii: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z},+,\cdot)$, $\mathbb{Z}[i]$

. Nu e integru dar e comutativ: $(\mathbb{Z}_{24},+,\cdot)$

$\hat{2}+\hat{17}=\hat{19}$
$\hat{3}\cdot\hat{4}=\hat{12}$
$\hat{4}\cdot\hat{6}=\hat{0}$

„Din cauza" lui $\hat{4},\hat{6}$ (și celelalte elemente care nu sunt prime cu 24), $\mathbb{Z}_{24}$ nu e integru

. Nici integru, nici comutativ: $M_n(\mathbb{R})$, $n \geq 2$ (vezi mai sus de ce)

2) a s.n. INVERSABIL LA STÂNGA (resp. LA DREAPTA) dacă $\exists b \in R$ a.î. $ab = 1$ (resp. $ba = 1$)

a s.n. INVERSABIL dacă e inv. la stg. și la dr, iar inversul său este a^{-1} și e unic

R s.n. CORP dacă orice element nenul al său e inversabil.

$U(R) = \{a \in R \mid a \text{ inversabil}\}$

. Practic, $(R,+,\cdot)$ corp $\Leftrightarrow$ $U(R) = R\setminus\{0\}$ $\Leftrightarrow$ $(R^*,\cdot)$ grup

Ex: $U(\mathbb{Z}) = \{\pm 1\}$
$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ (Revin cu o demonstrație)

Reguli de calcul: R inel

1) $a\cdot 0 = 0 \cdot a = 0$, $\forall a \in R$ (în $\mathbb{Z}$: $7777 \cdot 0 = 0$)
2) $a\cdot(-b) = (-a)b = -ab$, $a,b \in R$
3) Dacă $ab = ba$ și $n \in \mathbb{N}^*$ $\Rightarrow (a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$

Def: Fie R = inel, $S \subseteq R$. Spunem că S e SUBINEL al lui R dacă:

a) $1 \in S$

b) $x - y \in S$, $\forall\, x, y \in S$ (Practic, $(S, +)$ grup)

c) $xy \in S$, $\forall\, x, y \in S$

ex: $\mathbb{Z}$ subinel al lui $\mathbb{Q}$, subinel al lui $\mathbb{R}$, subinel al lui $\mathbb{C}$

$\mathbb{Z}[i]$ ...

Exerciții

① $A = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z},\ n \text{ impar} \right\}$ subinel în $(\mathbb{Q}, +, \cdot)$

SOL: 1) $1 \in S$ (E Trivial mam)

2) Fie $\frac{m_1}{n_1}, \frac{m_2}{n_2}$

$$\frac{m_1}{n_1} - \frac{m_2}{n_2} = \frac{\overbrace{(m_1 n_2 - m_2 n_1)}^{\in \mathbb{Z}}}{\underbrace{n_1 n_2}_{\in \mathbb{Z} \text{ și e impar}}} \in A$$

3) $\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} \in A$ (E Trivial mam)

Bonus: $U(A) = ?$

$\frac{m_1}{n_1}$ e inversabil $\Rightarrow \exists!\ \frac{m_2}{n_2} \in A$ a.î. $\frac{m_1 m_2}{n_1 n_2} = 1 \,/\cdot\, m_1 m_2 \neq 0$

$\Rightarrow m_1 m_2 = \underbrace{n_1 n_2}_{\text{impar}} \Rightarrow m_1 m_2$ impar $\Downarrow$ m_1, m_2 impare

Deci $U(A) = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z} \text{ impare} \right\}$

---

② $R = (\mathbb{Z} \times \mathbb{Q}, +, *)$, unde

$(a, x) * (b, y) = (ab, ay + bx)$

Convenție: $a, b, c \in \mathbb{Z}$, $x, y, z \in \mathbb{Q}$

Să vedem că R e inel, $U(R) = ?$, divizori ai lui zero

$*$ 4)

SOL: 1) $(\mathbb{Z}\times\mathbb{Q},+)$ grup abelian ✓

2) $(\mathbb{Z}\times\mathbb{Q},*)$ monoid

· $(a,x)*(b,y)=(ab,\ ay+bx)\in R$ (parte stabilă)

$\underbrace{}_{\in R}$ ✓

· asociativitate ✓

· elem. neutru: (e_1,e_2) elem. neutru $\Leftrightarrow$

$$(a,x)*(e_1,e_2)=(ae_1,\ ae_2+e_1x)=(a,x) \Rightarrow \begin{cases} ae_1=a, \forall a \\ ae_2+e_1x=x, \forall a,x \end{cases} \Rightarrow$$

$$\Rightarrow e_1=1$$
$$e_2=0$$

· $U(R)=?$

(a,x) inversabil $\Rightarrow \exists(c,z)$ a.î. $(a,x)*(c,z)=(1,0)$

$\Leftrightarrow (ac,\ az+cx)=(1,0)$

$\Leftrightarrow \begin{cases} ac=1 \\ az+cx=0 \end{cases} \overset{a,c\in\mathbb{Z}}{\Rightarrow} a=c=1$ sau $a=c=-1$

I $a=c=1 \Rightarrow z+x=0 \Rightarrow z=-x$

II $a=c=-1 \Rightarrow$

$* \ U(R)=\{(\pm1,x) \mid x\in\mathbb{Q}\}$

$(-1,x)*(-1,-x)=(1,\ \underbrace{x-x}_{0})=(1,0)$ Yey

(E comutativ?)

$(a,x)*(b,y)=(ab,\ ay+bx)$

$\qquad\qquad\qquad\qquad\qquad\qquad \shortparallel$

$(b,y)*(a,x)=(ab,\ bx+ay)$

3) Distributivitatea

$((a,x)+(b,y))*(c,z)=(a+b,\ x+y)*(c,z)=((a+b)c,\ (a+b)z+c(x+y))$

$(a,x)*(c,z)+(b,y)*(c,z)$

4) (a,x) divizor al lui zero $\Rightarrow \exists (b,y)\neq(0,0)$ a.î.

$(a,x)*(b,y)=(0,0) \Rightarrow (ab,\ ay+bx)=(0,0)$

$\Rightarrow \begin{cases} ab=0 \overset{b\neq0}{\Longrightarrow} \boxed{a=0} \\ ay+bx=0 \\ \quad bx \overset{b\neq0}{=} 0 \Rightarrow \boxed{x=0} \end{cases}$ Dar $(0,0)=0_R$

$\Downarrow$

integru

Integru + comutativ = Domeniu ♡

(3) A = inel comutativ finit, $a \in A \setminus \{0\}$ $(A,+,\cdot)$

Atunci $a \in U(A)$ sau a e divizor al lui zero.

SOL: Fie $a \in A \setminus \{0\}$ și presupunem că a NU e divizor al lui 0.

Caut o funcție injectivă care „îl pun în valoare pe a"

$\varphi_a : A \to A$, $\varphi_a(x) = ax$ injectivă

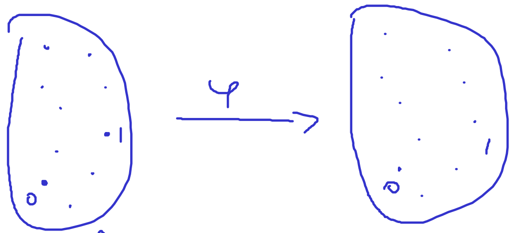
$$\left.\begin{array}{l}\varphi_a \text{ inj.}\\ A = \text{finit}\end{array}\right\} \Rightarrow \varphi_a \text{ bij.} \Rightarrow \exists x \in A \text{ a.î. } ax = 1$$

$$\Downarrow$$

$$a \in U(A)$$

OK

Ciorne



A_{inel} (finit) $\qquad$ A (finit)

Ce se întâmplă cu φ dacă φ e injectivă?

E bine, φ va fi bijectivă

$f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$, $f(x) = \hat{3}x$

$\hat{0} \xmapsto{f} \hat{0}$ $\qquad$ $\hat{6} \xmapsto{f} \hat{8}$

$\hat{1} \xmapsto{f} 3$ $\qquad$ $\hat{7} \xmapsto{f} \hat{1}$

$\hat{2} \xmapsto{f} 6$ $\qquad$ $\hat{8} \xmapsto{f} \hat{4}$

$\hat{3} \xmapsto{f} 9$ $\qquad$ $\hat{9} \xmapsto{f} \hat{7}$

$\hat{4} \xmapsto{f} 2$

$\hat{5} \xmapsto{f} 5$

Teorie: (izo)morfisme $\qquad$ R_1, R_2 inele

$f : R_1 \to R_2$ morfism dacă

$$f(x_1 + y_1) = f(x_1) + f(y_1)$$
$$f(x_1 \cdot y_1) = f(x_1) \cdot f(y_1)$$
$$f(1_{R_1}) = 1_{R_2}$$

f izomorfism $\Leftrightarrow$ f morfism bijectiv

Revin cu calculul pt. $U(\mathbb{Z}[i])$

Fie $a+bi \in U(\mathbb{Z}[i]) \Rightarrow \exists\ c+di \in \mathbb{Z}[i]$ a.î.

$(a+bi)(c+di)=1 \Rightarrow |a+bi|\cdot|c+di|=1$

$\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}=1 \quad / \ (\ )^2$ (ridic la pătrat)

$\underbrace{(a^2+b^2)}_{\in \mathbb{N}}\underbrace{(c^2+d^2)}_{\in \mathbb{N}}=1$

$\Rightarrow a^2+b^2=c^2+d^2=1$

$a^2+b^2=1 \Rightarrow a=\pm 1 \Rightarrow a+bi=\pm 1$

SAU

$b=\pm 1 \Rightarrow a+bi=\pm i$

Deci $U(\mathbb{Z}[i])=\{\pm 1, \pm i\}$