Curs 10 15.12.2020

Inele

Def 1. Un inel (unitar) este un triplet $(A,+,\cdot)$ format dintr-o mulțime nevidă A și 2 operații algebrice pe A, prima notată cu "+" și numită adunare, iar a doua notată cu "·" și numită înmulțire a.î.:

1) $(A,+)$ – grup abelian;
2) $(A,\cdot)$ – monoid;
3) $$\left.\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{aligned}\right\} (\forall)\, a,b,c\in A$$ (înmulțirea este distributivă față de adunare)

∴ Elementul neutru al adunării se notează cu 0; elementul neutru la înmulțire se notează cu 1. Inversul unui element $a\in A$ față de adunare se notează cu $-a$. Un element $a\in A$ s.n. inversabil dacă este inversabil față de înmulțire; în acest caz inversul său se notează cu a^{-1}.

∴ Notație. Mulțimea elementelor inversabile ale unui inel se notează cu $U(A)$, deci $U(A)=\{a\in A \mid (\exists)\, b\in A \text{ a.î. } a\cdot b=b\cdot a=1\}$.

∴ Inelul A s.n. nul dacă $A=\{0\}$. **Obs** Toate inelele cu care vom lucra sunt nenule. $(0\neq 1)$

Def 2 Un inel A s.n. <u>comutativ</u> dacă "$\cdot$" este comutativă.

Un inel A s.n. **corp** dacă orice element nenul este inversabil.

Exemple ① $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ — inele com.

$(\mathbb{Z}_n,+,\cdot)$ — inel com $(n\geq 2)$

com

(domeniu de integritate) inel care nu e corp $U(\mathbb{Z})=\{\pm 1\}\neq \mathbb{Z}^*$

corpuri

② $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ $\quad (\mathbb{Z}[i],+,\cdot)\to$ inel com (e domeniu de integritate) (vezi mai târziu)

inelul întregilor lui Gauss

③ $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$ $\quad (\mathbb{Z}[\sqrt{2}],+,\cdot)\to$ inel com (e domeniu de integritate)

④ **Exc!** $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$. Să se arate că $(\mathbb{Q}[\sqrt{2}],+,\cdot)$ este un corp com. ($(\mathbb{Q}[\sqrt{2}],+,\cdot)$ este inel com; fie $x=a+b\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$, $a,b\in\mathbb{Q}$

$x\neq 0 \Leftrightarrow a^2+b^2\neq 0$. $\quad \dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}=\underbrace{\dfrac{a}{a^2-2b^2}}_{\in\mathbb{Q}}\overset{\#}{0}+\underbrace{\dfrac{-b}{a^2-2b^2}}_{\in\mathbb{Q}}\cdot\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$)

$(x=0 \Leftrightarrow a=b=0)$

⑤ Fie $(A,+,\cdot)$ un inel.

$M_n(A)=\{(a_{ij})_{1\leq i,j\leq n} \mid a_{ij}\in A\ (\forall)\ i,j\in\{1,\dots,n\}\}$

mulțimea matricelor pătratice cu n linii și n coloane cu elemente din A

$$(a_{ij})_{1\le i,j\le n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ - & - & - & - \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{array}{l} \to \text{linia } 1 \\ \to \text{linia } 2 \\ \\ \to \text{linia } n \end{array}$$

$$0_{M_n(A)} = \begin{pmatrix} 0 & \cdots & 0 \\ - & - & - \\ 0 & \cdots & 0 \end{pmatrix} = O_n$$

$$1_{M_n(A)} = I_n$$

<u>Ex</u>! $(M_n(A), +, \cdot)$ este un inel, unde $+$, resp. $\cdot$, reprezintă operația uzuală de adunare, resp. înmulțire a matricelor.

Reamintesc

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

$$(a_{ij})_{1\le i,j\le n} \cdot (b_{ij})_{1\le i,j\le n} = (c_{ij})_{1\le i,j\le n}, \text{ unde}$$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}\cdot b_{nj} \; (\forall)\; i,j=\overline{1,n}.$$

<u>Obs</u> $(M_n(A), +, \cdot)$ este un inel necomutativ $(\forall)\; n\ge 2$.
(A inel nenul $(0\ne 1)$)

<u>Dem</u> $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ne \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

⑥ <u>Inelul de polinoame într-o nedeterminată cu coeficienți într-un inel (comutativ)</u>

Fie A inel comutativ nenul.

$A[X] = \{ a_0 + a_1 \cdot X + a_2 \cdot X^2 + \ldots + a_n \cdot X^n \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in A \}$.

inelul de pol. în nedeterminata X cu coeficienți în A în raport cu operațiile de adunare și înmulțire a polinoamelor definite astfel:

$$(a_0 + a_1 X + \ldots + a_n \cdot X^n) + (b_0 + b_1 X + \ldots + b_m X^m) = \begin{cases} (a_0+b_0) + (a_1+b_1)\cdot X + \ldots + (a_m+b_m)\cdot X^m + a_{m+1} X^{m+1} + \ldots + a_n X^n, & m \le n \\ (a_0+b_0) + (a_1+b_1)\cdot X + \ldots + (a_n+b_n)\cdot X^n + b_{n+1} X^{n+1} + \ldots + b_m X^m, & m > n \end{cases}$$

polinom

$$(a_0 + a_1 X + \ldots + a_n \cdot X^n) \cdot (b_0 + b_1 X + \ldots + b_m X^m) = c_0 + c_1 X + \ldots + c_{m+n} X^{m+n}$$

unde $c_k = \sum_{i+j=k} a_i b_j$. (*) $k = \overline{0, m+n}$.

Exemplu

$$(1 + 2x + 3x^2) \cdot (3 - 5x) = 3 - 5x + 6x - 10x^2 + 9x^2 - 15x^3 = 3 + x - x^2 - 15x^3.$$

Fie $f(X) = a_0 + a_1 X + \ldots + a_n X^n$ un polinom din $A[X]$ ($f(x) \in A[X]$)

grad(f) = cel mai mare nr. natural k a.î. $a_k \neq 0$ ($a_0, a_1, \ldots, a_n$ s.n. coeficienții polinomului) dacă $f(x) \neq 0$ și gradul polinomului nul at. $-\infty$.

Exemplu $f(x) = 1 - 2X + 3X^{2020}$ $\underline{\text{grad}(f) = 2020}$

$f(x) = 1 + 2X - 3X^2 + 0 \cdot X^3 + 0 \cdot X^4 = 1 + 2X - 3X^2$ $\underline{\text{grad}(f) = 2}$

Notatie Dacă $f(x) = a_0 + a_1 X + \ldots + a_n X^n$ și $a_n \neq 0$, atunci $\text{grad}(f) = n$, și a_n s.n. coeficientul dominant al lui $f(x)$.

Obs 1) Fie A un inel com și $f, g \in A[X] \setminus \{0\}$ (adică f, g sunt nenule).

Atunci: (a) $\text{grad}(f+g) \leq \max\{\text{grad}(f), \text{grad}(g)\}$.

(b) $\text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g)$ cu egalitate dacă și numai dacă produsul coeficienților dominanți ai lui f și g este nenul

2) $(A[X], +, \cdot)$ inel com. $0_{A[X]} = 0$ (polinomul nul)

$1_{A[X]} = 1$ (polinomul constant 1)

$A \subseteq A[X]$ deoarece $\underset{\overset{\cap}{A}}{a} = a + 0 \cdot X + \ldots + 0 \cdot X^n \in A[X]$.

Notatie De acum înainte $(A, +, \cdot)$ inel înseamnă inel comutativ nenul $(0 \neq 1)$

Def Fie A un inel (com). Un element $a \in A$ s.n. divizor al lui zero dacă există $x \in A, x \neq 0$ a.î. $a \cdot x = 0$.

• În orice inel nenul 0 este divizor al lui zero $(0\cdot 1 \overset{1)}{=} 0)$.

Reamintesc (Reguli de calcul într-un inel)
1) $0a = a\cdot 0 = 0$ $(\forall)\, a\in A$
2) $a\cdot(-b) = (-a)\cdot b = -ab$ $(\forall)\, a,b\in A$

• Un element inversabil nu este divizor al lui 0. (Dem $a\in U(A) \Rightarrow (\exists)\, b\in A$ a.î. $a\cdot b = 1$.
Dacă a este divizor al lui $0 \underset{def}{\Rightarrow} (\exists)\, c\in A, c\neq 0$ a.î. $a\cdot c = 0$.

$$\left.\begin{array}{l}(b\cdot a)c = 1\cdot c = c \\ \quad \| \\ b\cdot(a\cdot c) = b\cdot 0 \overset{1)}{=} 0\end{array}\right| \Rightarrow c = 0 \text{ ↯}$$

Deci a nu e divizor al lui zero.) $\Rightarrow 0\notin U(A)$.

Notație Notăm cu $D(A)$ mulțimea divizorilor lui 0 pentru un inel A.

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

Obs Un corp este un domeniu de integritate; reciproc nu e adevărat. De exemplu $\mathbb{Z}, \mathbb{Z}[i] \to$ domenii de integritate, dar nu sunt corpuri (Exc! $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$)

Teoremă Orice domeniu de integritate finit e corp.

Dem $(A,+,\cdot) \to$ domeniu de integritate finit $\Rightarrow$ $D(A) = \{0\}$, $|A| < \infty$.

Fie $a \in A \setminus \{0\}$ $f : A \longrightarrow A$ $f(x) = a \cdot x$ $(\forall)\, x \in A$

$\boxed{D(A) = \{0\}} \Longrightarrow f$ e injectivă

(Dem: $f(x) = f(y) \Rightarrow a \cdot x = a \cdot y \Rightarrow \underset{a \neq 0}{a \cdot (x-y) = 0} \Rightarrow x - y \in \underset{\{0\}}{D(A)}$
$\Rightarrow x = y$; f e inj)

$\left.\begin{array}{l} |A| < \infty \\ f \text{ inj} \end{array}\right| \Rightarrow f$ e bijectivă $\Rightarrow f$ e surjectivă $\Rightarrow (\exists)\, c \in A$ a.î. $\underset{a \cdot c}{f(c)} = 1 \Rightarrow$

$\Rightarrow a \in U(A)$. Deci A e corp. ▢

Exc 1 $U(\mathbb{Z}_n) = \{\hat{x} \mid x \in \mathbb{Z}, (x, n) = 1\}$ $D(\mathbb{Z}_n) = \mathbb{Z}_n \setminus U(\mathbb{Z}_n)$!

Exc 2 Fie $n \geq 2$. $\mathbb{Z}_n$ e corp $\Longleftrightarrow n$ e număr prim.

Def. Fie A un inel. Atunci o submulțime nevidă B a lui A s.n. subinel al lui A dacă:
1) $(B, +) \leq (A, +)$
2) $a \cdot b \in B$ $(\forall)\, a \in B, b \in B$
3) $1 \in B$.

• O submulțime nevidă I a lui A s.n. ideal dacă: 1) $(I, +) \leq (A, +)$
2) $a \cdot x \in I$ $(\forall)\, a \in A$ $(\forall)\, x \in I$

Obs 1) Idealele lui $(\mathbb{Z}, +, \cdot)$ sunt $n\mathbb{Z}$.
Un inel ~~nenul~~ Aerit comp $\Longleftrightarrow$ are exact 2 ideale (0) și A.
3)

2) Orice inel A are 2 ideale: (0) și A.
(nenul)