CURS 2

Două inele importante

Reamintim din cursul anterior: $(R, +, \cdot)$ este **inel** dacă:
i) $(R, +)$ este grup abelian;
ii) Operaţia $\cdot$ este asociativă;
iii) Operaţia $\cdot$ este distributivă faţă de $+$, adică

$$a(b+c) = ab + ac \text{ şi } (b+c)a = ba + ca,\ \forall a, b, c \in \mathbb{R}.$$

Inelul $(R, +, \cdot)$ se numeşte **comutativ**, respectiv **cu unitate** dacă operaţia $\cdot$ este comutativă, respectiv dacă are element unitate (notat cu 1). Dacă $(R, +, \cdot)$ este un inel cu unitate, atunci un element $a \in R$ se numeşte **inversabil** dacă

$$\exists\ a^{-1} \in R:\ a^{-1}a = 1 = aa^{-1}. \tag{1}$$

Fie $(R, +, \cdot)$ şi $(R', +, \cdot)$ două inele. O funcţie $f : R \to R'$ se numeşte **morfism** (sau **omomorfism**) **de inele** dacă pentru orice $x_1, x_2 \in R$,

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ şi } f(x_1 x_2) = f(x_1) f(x_2). \tag{2}$$

Un morfism bijectiv de inele se numeşte **izomorfism (de inele)**. Un morfism al lui $(R, +, \cdot)$ în el însuşi se numeşte **endomorfism al inelului** $(R, +, \cdot)$. Un izomorfism al lui $(R, +, \cdot)$ pe el însuşi se numeşte **automorfism al inelului** $(R, +, \cdot)$. Dacă există un izomorfism $f : R \to R'$, atunci se spune că inelele $(R, +, \cdot)$ şi $(R', +, \cdot)$ sunt **izomorfe** şi vom scrie $R \simeq R'$ sau $(R, +, \cdot) \simeq (R', +, \cdot)$.

Fie $(R, +, \cdot)$ şi $(R', +, \cdot)$ inele cu unitate (1 şi $1'$ fiind, respectiv, unităţile lor). Un **morfism** $f : R \to R'$ se numeşte **unital** dacă

$$f(1) = 1' \tag{3}$$

Exemplele 1. a) Dacă $(R, +, \cdot)$ şi $(R', +, \cdot)$ sunt inele, atunci funcţia $\theta : R \to R'$, $\theta(x) = 0$ este un morfism numit **morfismul nul** sau **zero**. Dacă R şi R' sunt cu unitate şi $|R'| \geq 2$, atunci morfismul θ nu este unital.
b) Fie $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (unde $\overline{z}$ este conjugatul lui z). Din

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} \text{ şi } \overline{\overline{z}} = z$$

rezultă că f este un automorfism al corpului $(\mathbb{C}, +, \cdot)$ şi $f^{-1} = f$.

Prima condiţie din (2) arată că dacă $f : R \to R'$ este un morfism între inelele $(R, +, \cdot)$ şi $(R', +, \cdot)$, atunci f este morfism al grupului $(R, +)$ în $(R', +)$ prin urmare, avem:

Teorema 2. Fie $(R, +, \cdot)$, $(R', +, \cdot)$ inele şi $f : R \to R'$ un morfism. Atunci

$$f(0) = 0 \text{ şi } f(-x) = -f(x),\ \forall\ x \in R. \tag{4}$$

Dacă R şi R' sunt inele cu unitate, f este morfism unital şi $x \in R$ e inversabil, atunci

$$f(x^{-1}) = [f(x)]^{-1}. \tag{5}$$

Demonstraţie. Morfismele de grupuri păstrează elementul neutru şi duc simetricul unui element în simetricul imaginii sale, de unde rezultă (4). Din

$$xx^{-1} = 1 = x^{-1}x$$

şi din (3) urmează

$$f(x)f(x^{-1}) = 1' = f(x^{-1})f(x)$$

ceea ce demonstrează pe (5). □

Observaţia 3. Orice morfism nenul dintre două corpuri este unital.

Într-adevăr, dacă $(K, +, \cdot)$ şi $(K', +, \cdot)$ sunt corpuri, iar $f : K \to K'$ este un morfism nenul, atunci există $x_0 \in K$ astfel încât $f(x_0) \neq 0$. Cum

$$1 \cdot x_0 = x_0 \Rightarrow f(1)f(x_0) = f(x_0) = 1'f(x_0),$$

înmulţind la dreapta ambii membri cu inversul lui $f(x_0)$ în K', obţinem $f(1) = 1'$.

Inelul polinoame cu coeficienţi într-un corp comutativ

Fie $(K, +, \cdot)$ un corp comutativ. Fie $K^{\mathbb{N}}$ mulţimea şirurilor cu termenii din K, adică

$$K^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to K\}.$$

Dacă $f : \mathbb{N} \to K$ atunci notând $f(n) = a_n$ scriem

$$f = (a_0, a_1, a_2, \dots).$$

Pentru $f = (a_0, a_1, a_2, \dots)$, $g = (b_0, b_1, b_2, \dots) \in K^{\mathbb{N}}$ se definesc:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \tag{1}$$

$$f \cdot g = (c_0, c_1, c_2, \dots) \tag{2}$$

unde

$$\begin{aligned}
c_0 &= a_0 b_0, \\
c_1 &= a_0 b_1 + a_1 b_0, \\
&\vdots \\
c_n &= a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0 = \sum_{i+j=n} a_i b_j, \\
&\vdots
\end{aligned}$$

Teorema 4. $K^{\mathbb{N}}$ formează în raport cu operaţiile definite în (1) şi (2) un inel comutativ şi cu unitate numit **inelul seriilor formale** cu coeficienţi din K.

Demonstraţie. TEMĂ el. nul: $(0,0,\dots)$; el. unitate: $(1,0,0,\dots)$ □

Fie $f = (a_0, a_1, a_2, \dots) \in K^{\mathbb{N}}$. Se numeşte **suportul lui** f submulţimea lui $\mathbb{N}$

$$supp\, f = \{k \in \mathbb{N} \mid a_k \neq 0\}.$$

Notăm cu $K^{(\mathbb{N})}$ submulţimea lui $K^{\mathbb{N}}$ formată din şirurile de **suport finit**. Deci

$$f \in K^{(\mathbb{N})} \Leftrightarrow \exists\, n \in \mathbb{N} \text{ astfel încât } a_i = 0 \text{ pentru } i \geq n \Leftrightarrow f = (a_0, a_1, a_2, \dots, a_{n-1}, 0, 0, \dots).$$

$supp\, f \subseteq \{0, 1, \dots, n-1\}$

Teorema 5. i) $K^{(\mathbb{N})}$ este un subinel al lui $K^{\mathbb{N}}$ ce conţine unitatea.
ii) Funcţia $\varphi : K \to K^{(\mathbb{N})}$, $\varphi(a) = (a, 0, 0, \dots)$ este un omomorfism unital injectiv de inele.

Demonstraţie.

i) $f = (a_0, a_1, \dots, a_k, 0, 0, \dots) \in K^{(\mathbb{N})}$
$g = (b_0, b_1, \dots, b_k, 0, 0, \dots) \in K^{(\mathbb{N})}$

$f + g = (a_0 + b_0, \dots, a_k + b_k, 0, 0, \dots) \in K^{(\mathbb{N})}$
$\Rightarrow K^{(\mathbb{N})}$ $\neq$. s. în $(K^{\mathbb{N}}, +)$

$f = (a_0, a_1, \dots, a_n, 0, \dots)$, $g = (b_0, b_1, \dots, b_m, 0, \dots)$

$fg = (c_0, c_1, \dots, c_k, \dots, c_{m+n}, 0, 0, \dots) \in K^{(\mathbb{N})}$

Într-adevăr,

$$k > m+n \Rightarrow c_k = \sum_{i+j=k} a_i b_j = a_0 \underset{0}{\underbrace{b_k}} + a_1 \underset{0}{b_{k-1}} + \dots + a_n \underset{0}{b_{k-n}} + \overset{0}{a_{n+1}} b_{k-n-1} + \dots + \overset{0}{a_{k-m}} b_m + \dots + \overset{0}{a_k} b_0 = 0$$

$\Rightarrow (K^{(\mathbb{N})}, \underset{\text{op. indusă}}{+})$ grup abelian; $(0, 0, \dots, 0, \dots) \in K^{(\mathbb{N})}$

$f \in K^{(\mathbb{N})} \overset{?}{\Longrightarrow} -f \in K^{(\mathbb{N})}$ (temă)

„$\cdot$" distr. față de „$+$" în $K^{(\mathbb{N})}$

$(K^{(\mathbb{N})}, \underset{\text{op. indusă}}{\cdot})$ monoid com. $(1, 0, 0, \dots) \in K^{(\mathbb{N})}$

Deci $(K^{(\mathbb{N})}, +, \cdot)$ inel com. cu unitate

ii) $\varphi(a+b) = (a+b, 0, \dots) = (a, 0, \dots) + (b, 0, \dots) = \varphi(a) + \varphi(b)$
$\varphi(ab) = (ab, 0, 0, \dots) = (a, 0, \dots, 0, \dots)(b, 0, \dots) = \varphi(a)\varphi(b)$
$\forall a, b \in K$ Deci φ morfism de inele.

$\varphi(1) = (1, 0, \dots) \Longrightarrow \varphi$ unital

$a, b \in K$, $\varphi(a) = \varphi(b) \Longleftrightarrow (a, 0, \dots) = (b, 0, \dots) \Rightarrow a = b$ (φ inj.)

$\underline{\varphi : K \to \varphi(K)} = \{(a, 0, 0, \dots) \mid a \in K\}$
izomorfism

Identificare a cu $(a, 0, 0, \dots)$

Inelul $(K^{(\mathbb{N})}, +, \cdot)$ se numeşte **inelul polinoamelor** cu coeficienţi din K. Cum ajunge el să ,,arate" aşa cum îl ştim din liceu?

Omomorfismul injectiv φ ne permite să identificăm elementul $a \in K$ cu polinomul $(a, 0, 0, \dots)$. După această identificare K devine subinel al inelului $K^{(\mathbb{N})}$. Polinomul

$$X = (0, 1, 0, 0, \dots) \notin K$$

se numeşte **nedeterminată** peste K. Din (2) rezultă:

$$\begin{aligned} X^2 &= (0, 0, 1, 0, 0, \dots) \\ X^3 &= (0, 0, 0, 1, 0, 0, \dots) \\ &\vdots \\ X^m &= (\underbrace{0, 0, \dots, 0}_{m\ ori}, 1, 0, 0, \dots) \\ &\vdots \end{aligned}$$

Identificând pe $a \in K$ cu $(a, 0, 0, \dots)$, din (2) urmează

$$aX^m = (\underbrace{0, 0, \dots, 0}_{m\ ori}, a, 0, 0, \dots) \tag{3}$$

şi astfel, $f = (a_0, a_1, \dots, a_m, 0, 0, \dots) = a_0 + a_1 X + \dots + a_m X^m$

Teorema 6. Orice $f \in K^{(\mathbb{N})}$ nenul se scrie în mod unic sub forma

$$f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \tag{4}$$

numită **forma algebrică** a lui f, unde $a_i \in K$, $i \in \{0, 1, \dots, n\}$ cu $a_n \neq 0$.

Acum putem rescrie

$$K^{(\mathbb{N})} = \{f = a_0 + a_1 X + \dots + a_n X^n \mid a_0, a_1, \dots, a_n \in K,\ n \in \mathbb{N}\} \overset{not}{=} K[X].$$

Pentru un element al acestei mulţimi folosim şi numele **polinom cu coeficienţi din** K **în nedeterminata** X, iar pentru $K[X]$ mulţimea sau inelul polinoamelor cu coeficienţi în corpul K în nedeterminata X. De asemenea, putem rescrie operaţiile din inelul $(K[X], +, \cdot)$ aşa cum le ştim din liceu (la seminar).

Dacă $f \in K[X]$, $f \neq 0$ şi f are reprezentarea (4), atunci n se numeşte **gradul lui** f, iar dacă $f = 0$ atunci se spune că f are gradul $-\infty$. Gradul lui f îl vom nota cu $grad\, f$. Rezultă că

$$grad\, f = 0 \Leftrightarrow f \in \cancel{K}. \ K \setminus \{0\}$$

Luăm prin definiţie

$$-\infty + m = m + (-\infty) = -\infty,\ -\infty + (-\infty) = -\infty,\ -\infty < m,\ \forall\, m \in \mathbb{N}.$$

Au loc următoarele:

i) $grad\,(f + g) \leq \max\{grad\, f, grad\, g\}, \forall f, g \in K[X]$;

ii) $grad\,(fg) = grad\, f + grad\, g, \forall f, g \in K[X]$;

iii) $K[X]$ este domeniu de integritate (la seminar);
iv) un polinom $f \in K[X]$ este inversabil în $K[X]$ dacă şi numai dacă $f \in K^*$ (la seminar).

Câteva noţiuni şi proprietăţi utile referitor la polinoame:
Dacă $f, g \in K[X]$ atunci

$$f \mid g \Leftrightarrow \exists\ h \in \cancel{K}\, K[X],\ g = fh.$$

Relaţia de divizibilitate $\mid$ este o relaţie reflexivă şi tranzitivă în $K[X]$. Polinomul nul se comportă faţă de aceste relaţii astfel:

$$f \mid 0,\ \forall f \in K[X] \text{ şi } \nexists f \in K[X] \setminus \{0\} :\ 0 \mid f.$$

Două polinoame $f, g \in K[X]$ sunt **asociate în divizibilitate** (scriem $f \sim g$) dacă avem

$$\exists\ a \in K^* :\ f = ag.$$

Relaţia de asociere în divizibilitate $\sim$ este o relaţie de echivalenţă pe $K[X]$.

Un **polinom** $f \in K[X]^*$ se numeşte **ireductibil** dacă $grad\, f \geq 1$ şi

$$f = gh\ (g, h \in K[X]) \Rightarrow g \in K^* \text{ sau } h \in K^*.$$

Noţiunile de c.m.m.d.c. şi c.m.m.m.c. se definesc ca în cazul numerelor întregi, produsul c.m.m.d.c. cu c.m.m.m.c. a două polinoame este asociat în divizibilitate cu produsul polinoamelor, iar comportamentul relaţiei de divizibilitate faţa de sumă şi produs este similar cu cel pe care îl cunoaştem de la numere întregi.

Dacă $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$ şi $c \in K$, atunci

$$f(c) = a_0 + a_1c + a_2c\cancel{X}^2 + \cdots + a_nc^n \in K$$

se numeşte **imaginea polinomului** f **în (punctul)** c. Elementul $c \in K$ se numeşte **rădăcină a lui** f dacă $f(c) = 0$.

Teorema 7. (Teorema împărţirii cu rest în $K[X]$) Pentru orice polinoame $f, g \in K[X]$, $g \neq 0$, există două polinoame unice $q, r \in K[X]$ astfel încât

$$f = gq + r \text{ şi } grad\, r < grad\, g. \tag{5}$$

Demonstraţie. (facultativ) Fie $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$, $b_m \neq 0$ şi

$$f = a_0 + a_1X + \cdots + a_nX^n \text{ şi } g = b_0 + b_1X + \cdots + b_mX^m.$$

Existenţa polinoamelor q şi r: Dacă $f = 0$ atunci $q = r = 0$ verifică (5).

Pentru $f \neq 0$ procedăm prin inducţie după $n = \operatorname{grad} f$. Dacă $n < m$ (întrucât $m \geq 0$ există polinoame f care verifică această condiţie), atunci $q = 0$ şi $r = f$ verifică pe (5).

Presupunem afirmaţia adevărată pentru polinoamele de grad mai mic decât $n \geq m$. Cum a_nX^n este termenul de grad maxim al polinomului $a_nb_m^{-1}X^{n-m}g$, pentru polinomul $h = f - a_nb_m^{-1}X^{n-m}g$, avem $\operatorname{grad} h < n$ şi conform ipotezei există $q', r \in R[X]$ astfel încât

$$h = gq' + r \text{ şi } \operatorname{grad} r < \operatorname{grad} g.$$

Rezultă că $f = h + a_nb_m^{-1}X^{n-m}g = (a_nb_m^{-1}X^{n-m} + q')g + r = gq + r$ unde $q = a_nb_m^{-1}X^{n-m} + q'$. Deci existenţa polinoamelor q şi r care verifică pe (5) este demonstrată.

Unicitatea polinoamelor q şi r: Dacă mai avem

$$f = gq_1 + r_1 \text{ şi } \operatorname{grad} r_1 < \operatorname{grad} g,$$

atunci $gq + r = gq_1 + r_1$ de unde rezultă $r - r_1 = g(q_1 - q)$ şi $\operatorname{grad}(r - r_1) < \operatorname{grad} g$. Întrucât $g \neq 0$ urmează $q_1 - q = 0$ ceea ce implică $r - r_1 = 0$, adică $q_1 = q$ şi $r_1 = r$. $\square$

Polinoamele q şi r din (5) se numesc **câtul**, respectiv **restul** împărţirii lui f la g.

Corolarul 8. Fie K este un corp comutativ şi $c \in K$. Atunci restul împărţirii unui polinom $f \in K[X]$ la polinomul $X - c$ este $f(c)$.

Într-adevăr, din (5) rezultă că restul r al împărţirii lui f la $X - c$ este un element din K, iar cum $f = (X - c)q + r$, se deduce că $r = f(c)$. Cazul $r = 0$ ne conduce imediat la:

Corolarul 9. Fie K este un corp comutativ. Un element $c \in K$ este rădăcină a lui f dacă şi numai dacă $(X - c) \mid f$.

$\in \mathbb{N}$

Corolarul 10. Dacă K este un corp comutativ, atunci un polinom nenul $f \in K[X]$ de grad k are cel mult k rădăcini în K.

Într-adevăr pentru polinoamele de gradul zero afirmaţia este adevărată deoarece polinoamele de gradul zero nu au rădăcini. Presupunem $k > 0$ şi afirmaţia adevărată pentru polinoamele de grad mai mic decât k. Dacă $c_1 \in K$ este rădăcină a lui f, atunci $f = (X - c_1)q$ şi $\operatorname{grad} q = k - 1$. Conform ipotezei, polinomul q are cel mult $k-1$ rădăcini în K. Cum K este corp comutativ, $K[X]$ este domeniu de integritate şi din $f = (X - c_1)q$ rezultă că $c \in K$ este rădăcină a lui f dacă şi numai dacă $c = c_1$ sau c este rădăcină lui q. Deci f are cel mult k rădăcini în K.

Inelul matricilor pătrat(ic)e cu elemente într-un corp comutativ

Fie K o mulţime şi $m, n \in \mathbb{N}^*$. O funcţie

$$A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to K$$

se numeşte **matrice** de tipul (m, n) cu elemente din K. Când $m = n$ matricea A se numeşte **matrice pătratică** de ordinul n. Notând pentru toţi $i = 1, \ldots, m$ şi $j = 1, \ldots, n$ pe $A(i, j)$ cu $a_{ij} (\in K)$, putem scrie pe A sub formă de tabel dreptunghiular cu m linii şi n coloane în care trecem imaginea fiecărei perechi (i, j) în linia i şi coloana j

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Pentru acest tabel vom folosi notaţia

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

sau, mai simplu, $A = (a_{ij})$. Mulţimea matricelor de tipul (m, n) cu elemente din K o vom nota cu $M_{m,n}(K)$, iar când $m = n$ cu $M_n(K)$.

Fie $(K,+,\cdot)$ este un corp comutativ. Atunci $+$ din K determină o operaţie $+$ în $M_{m,n}(K)$ definită astfel: dacă $A=(a_{ij})$ şi $B=(b_{ij})$ sunt două matrice de tipul (m,n) atunci

$$A+B=(a_{ij}+b_{ij}).$$

Se verifică uşor că această operaţie este asociativă, comutativă, are ca element neutru (element nul) matricea $O_{m,n}$ care are pe 0 în toate poziţiile (numită **matricea nulă**) şi fiecare element $A=(a_{ij})$ din $M_{m,n}(K)$ are un opus (pe matricea $-A=(-a_{ij})$, numită **opusa matricei** A). Aşadar,

Teorema 11. $(M_{m,n}(K),+)$ este un grup abelian.

Înmulţirea unei matrici $A=(a_{ij})\in M_{m,n}(K)$ cu un scalar $\alpha\in K$ este definită astfel:

$$\alpha A=(\alpha a_{ij}).$$

Se verifică uşor că aceasta are următoarele proprietăţi:

i) $\alpha(A+B)=\alpha A+\alpha B,\ \forall\alpha\in K,\ \forall A,B\in M_{m,n}(K)$;

ii) $(\alpha+\beta)A=\alpha A+\beta A,\ \forall\alpha,\beta\in K,\ \forall A\in M_{m,n}(K)$; (TEMĂ)

iii) $(\alpha\beta)A=\alpha(\beta A),\ \forall\alpha,\beta\in K,\ \forall A\in M_{m,n}(K)$;

iv) $1\cdot A=A,\ \forall A\in M_{m,n}(K)$.

Înmulţirea matricelor este definită astfel: dacă $A=(a_{ij})\in M_{m,n}(K)$ şi $B=(b_{ij})\in M_{n,p}(K)$, atunci

$$AB=(c_{ij})\in M_{m,p}(K),\ \text{cu } c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\ (i,j)\in\{1,\dots,m\}\times\{1,\dots,p\}.$$

Să considerăm pentru $n\in\mathbb{N}^*$ matricea (pătratică) de tipul (n,n):

$$I_n=\begin{pmatrix}1&0&0&\dots&0\\0&1&0&\dots&0\\\vdots&\vdots&\vdots&\dots&\vdots\\0&0&0&\dots&1\end{pmatrix}.$$

Dacă $m,n,p,q\in\mathbb{N}^*$, atunci:

1) $(AB)C=A(BC)$, pentru orice matrice $A\in M_{m,n}(K),\ B\in M_{n,p}(K),\ C\in M_{p,q}(K)$;

2) $I_mA=A=AI_n,\ \forall A\in M_{m,n}(K)$;

3) $A(B+C)=AB+AC$ pentru orice matrice $A\in M_{m,n}(K),\ B,C\in M_{n,p}(K)$;

3') $(B+C)D=BD+CD$, pentru orice $B,C\in M_{n,p}(K),\ D\in M_{p,q}(K)$;

4) $\alpha(AB)=(\alpha A)B=A(\alpha B),\ \forall\alpha\in K,\ \forall A_{m,n}(K),\ \forall B\in M_{n,p}(K)$.

Demonstrăm ca exemplu pe 1). Celelalte egalităţi fiind mai uşor de demonstrat rămân TEMĂ. Într-adevăr, dacă $A=(a_{ij})\in M_{m,n}(K),\ B=(b_{ij})\in M_{n,p}(K),\ C=(c_{ij})\in M_{p,q}(K)$, atunci elementul din linia $i\in\{1,\dots,m\}$ şi coloana $l\in\{1,\dots,q\}$ a produsului $(AB)C$ este

$$\sum_{j=1}^{p}\left(\sum_{k=1}^{n}a_{ik}b_{kj}\right)c_{jl}=\sum_{j=\overline{1,p},k=\overline{1,n}}(a_{ik}b_{kj})\,c_{jl}=\sum_{j=\overline{1,p},k=\overline{1,n}}a_{ik}\,(b_{kj}c_{jl})=\sum_{k=1}^{n}a_{ik}\left(\sum_{j=1}^{p}b_{kj}c_{jl}\right),$$

care este elementul din linia $i\in\{1,\dots,m\}$ şi coloana $l\in\{1,\dots,q\}$ a produsului $A(BC)$.

Dacă lucrăm cu matrici pătratice de acelaşi ordin n, înmulţirea $\cdot$ de mai sus devine o lege de compoziţie (operaţie) pe $M_n(K)$, iar din egalităţile 1)–3') deducem că $\cdot$ este asociativă, că I_n este element neutru (unitate) faţă de $\cdot$ (motiv pentru care o şi numim **matricea unitate** de ordinul n) şi că $\cdot$ este distributivă faţa de $+$. Aşadar,

Teorema 12. $(M_n(K), +, \cdot)$ este un inel cu unitate numit **inelul matricelor pătrat(ic)e de ordinul** n **cu elemente din** K.

Observaţiile 13. a) Dacă $n \geq 2$ atunci inelul $M_n(K)$ nu este comutativ şi are divizori ai lui zero. Dacă $a, b \in K^*$, atunci matricele nenule

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \dots & b \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

pot fi folosite atât pentru a demonstra că $M_n(K)$ are divizori ai lui zero, cât şi pentru a arăta că semigrupul $(M_n(K), \cdot)$ nu este comutativ.
b) Din proprietăţile adunării, înmulţirii şi înmulţirii cu scalari a matricelor, rezultă că funcţia

$$f : K \to M_n(K),\ f(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix} = aI_n$$

unital

este un omomorfism injectiv de inele.

Transpusa unei matrice $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = (a_{ij})$ de tipul (m, n) este matricea de tipul (n, m),

$${}^tA = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \dots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix} = (a_{ji}).$$

Modul în care transpusa se comportă faţa de adunare, înmulţire şi înmulţirea cu scalari rezultă din egalităţile:

${}^t(A + B) = {}^tA + {}^tB,\ \forall A, B \in M_{m,n}(K);$
${}^t(AB) = {}^tB \cdot {}^tA,\ \forall A \in M_{m,n}(K),\ \forall B \in M_{n,p}(K);$
${}^t(\alpha A) = \alpha \cdot {}^tA,\ \forall A \in M_{m,n}(K).$

Fie K un corp comutativ. Mulţimea elementelor inversabile ale inelului $M_n(K)$ este

$$GL_n(K) = \{A \in M_n(K) \mid \exists B \in M_n(K) : AB = BA = I_n\}.$$

Mulţimea $GL_n(K)$ e stabilă în $(M_n(K), \cdot)$ şi $(GL_n(K), \cdot)$ e un grup numit **grupul general liniar de gradul** n peste K. Se ştie că dacă K este unul dintre corpurile numerice ($\mathbb{Q}$, $\mathbb{R}$ sau $\mathbb{C}$) atunci $A \in M_n(K)$ este inversabilă dacă şi numai dacă $\det A \neq 0$. Prin urmare,

$$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A \neq 0\},$$

şi analog se pot redefini şi $GL_n(\mathbb{R})$ şi $GL_n(\mathbb{Q})$. Vom vedea că la fel se întâmplă în orice inel $M_n(K)$ cu K corp comutativ. Ca atare, urmează să discutăm despre **determinantul unei matrice pătratice cu elemente într-un corp comutativ** K.