

Complemente de spații vectoriale

Peste tot în aceste lecții K este un corp comutativ.

Orice sp. vet. V de dimensiune n este izomorf cu K^n , izomorfismul fiind dat de aplicția lineară constituită astfel: fie $B = \{e_1, \dots, e_n\}$ o bază a lui V . Orice $v \in V$ se scrie ca o combinație liniară

$$v = d_1 e_1 + d_2 e_2 + \dots + d_n e_n, \quad d_i \in K,$$

cu scalarii d_1, \dots, d_n unic determinați. Astăzi, vectorul

$$(v)_B := (d_1, d_2, \dots, d_n) \in K^n$$

este, la rândul său, unic determinat. Atunci, aplicția liniară

$$\varphi: V \longrightarrow K^n, \quad \varphi: v \longmapsto (v)_B$$

este bine definită și este un izomorfism de spații vectoriale.

Legătura $v \longleftrightarrow (v)_B$, intermediată de bază B , face ca din punct de vedere structural K^n să fie o reprezentare convenabilă a lui V .

(1) EXEMPLU. Multimea $B = \{E_1, E_2, E_3, E_4\}$, unde $E_1 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$, $E_2 = \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}$,

$E_3 = \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}$, $E_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ este o bază a lui $V = M_2(\mathbb{R})$ peste \mathbb{R} . Deoarece

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = aE_1 + (a+b)E_2 + (a-c)E_3 + (b+c+d)E_4,$$

aplicația $\varphi: M_2(\mathbb{R}) \longrightarrow \mathbb{R}^4$ are legătură de corespondență

$$\varphi: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto (a, a+b, a-c, b+c+d) = (v)_B$$

iar inversa $\psi: \mathbb{R}^4 \longrightarrow M_2(\mathbb{R})$ este dată de corespondență

$$\psi: (x_1, x_2, x_3, x_4) \longmapsto x_1 E_1 + x_2 E_2 + x_3 E_3 + x_4 E_4 = \begin{pmatrix} x_1 & -x_1 + x_2 \\ x_3 & x_1 - x_2 + x_3 + x_4 \end{pmatrix} = v$$

Să verificăm rel. $\varphi \circ \psi = 1_{M_2(\mathbb{R})}$ și $\psi \circ \varphi = 1_{\mathbb{R}^4}$ pe un caz particular.

Amen

$$\begin{pmatrix} 2 & 3 \\ -4 & 1 \end{pmatrix} \xrightarrow{\varphi} (2, 5, 6, 0) \xrightarrow{\psi} \begin{pmatrix} 2 & 3 \\ -4 & 1 \end{pmatrix}$$

$$\xrightarrow{\psi} \begin{pmatrix} 2 & 3 \\ -4 & 1 \end{pmatrix} \xrightarrow{\varphi} (2, 5, 6, 0)$$

In definitiv, de acum înainte vom lucra numai pe A.V. K .

Baze pentru subspații generate

Fie $v_1, v_2, \dots, v_m \in K^n$, respectiv

$$v_1 = (a_{11}, a_{12}, \dots, a_{1n})$$

$$v_2 = (a_{21}, a_{22}, \dots, a_{2n})$$

$$v_m = (a_{m1}, a_{m2}, \dots, a_{mn})$$

Cu acești vectori construim matricea

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_m \end{pmatrix} \quad (1)$$

în care vectorii devin linile matricei A. În acest fel, subspațiul

$$W = L(v_1, \dots, v_m) = L(l_1, \dots, l_m) \text{ not } \text{sphin}(A),$$

și numim spatiu liniilor lui A.

(2) PROP. $\text{sphin}(A)$ este invariant față de operăriile elementare pe linii asupra matricei A, avem:

(a) $\text{sphin}(A)$ este invariant de interzimbarea a două lini, adică

$$L(l_1, \dots, l_i, \dots, l_j, \dots, l_m) = L(l_1, \dots, l_j, \dots, l_i, \dots, l_m), \quad i < j.$$

(b) $\text{sphin}(A)$ este invariant dacă o linie e înmulțită cu un scalar nenul, adică,

$$L(l_1, \dots, l_i, \dots, l_m) = L(l_1, \dots, \lambda l_i, \dots, l_m), \quad \forall \lambda \in K^*.$$

(c) $\text{sphin}(A)$ este invariant dacă la o linie adunăm o altă linie înmulțită cu un scalar, adică

$$L(l_1, \dots, l_i, \dots, l_j, \dots, l_m) = L(l_1, \dots, l_i + \lambda l_j, \dots, l_j, \dots, l_m), \quad \forall \lambda \in K, i \neq j.$$

Dem. (Indicativ). Egalitățile se demonstrează prin dublu inclusiune. Este suf. să arătăm că fiecare din generatorii suntează din subspații se află în cetele subspațiu. ■

(3) COROLAR. Pentru orice matrice $A \in M_{m,n}(K)$ spațiul vectorial $\text{sphin}(A)$ este invariant față de orice sir de oper. elem. pe linii efectuate asupra lui A. ■

Scopul oper. elem. pe linii este de a obține o formă echivalentă pe linii, adică o

matrice $A' = (a'_{ij})$, $1 \leq i \leq m, 1 \leq j \leq n$ de forma

$$A' = \begin{pmatrix} a'_{11} & \cdots & \cdots & \cdots & a'_{1m} \\ 0 & \cdots & 0 & a'_{2j_1} & \cdots & \cdots & a'_{2n} \\ \vdots & \ddots & 0 & 0 & \cdots & 0 & a'_{rj_r} & \cdots & a'_{rn} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 \end{pmatrix} = \begin{pmatrix} L'_1 \\ L'_2 \\ \vdots \\ L'_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (2)$$

In care

(i) primele r linii sunt nemele, iar următoarele $m-r$ linii sunt nule;

(ii) linia L'_i are forma

$$L'_i = (0, \dots, 0, a'_{ij_1}, a'_{ij_2}, \dots, a'_{ij_r}, \dots, a'_{im}) \rightarrow \text{cu } a'_{ij_i} \neq 0.$$

$$(iii) 1 < j_2 < j_3 < \dots < j_r \leq m.$$

Elem. nemele $a'_{11}, a'_{2j_2}, \dots, a'_{rj_r}$ sunt pivoti.

(4) OBS. Pt. simplitate și fără a afecta generalitatea se presupune că prima coloană a matr. A conține elem. nemele, motiv că cu $a'_{11} \neq 0$. Atât, primul element nemul de pe linie anterioară a lui A' , nume a'_{ij_1} , este și el precedat de câteva zeroi.

(5) PROP. Pentru orice matrice $A \in M_{m,n}(k)$ se poate construi o formă escalonată A' de forma (2) folosind următorul algoritm:

Pasul 1. Se interzchimbă, eventual, linia 1 cu o altă linie pentru a obține $a_{11} \neq 0$.

Pasul 2. Pentru $i > 0$, linia L'_i se transformă în formula

$$L'_i := a_{11}L'_i - a_{i1}L_1$$

care este succesiunea operațiilor $L'_i := L_i - \frac{a_{i1}}{a_{11}}L_1$ și $L'_i = a_{11}L_i$,

c.f. schema:

$$\left(\begin{array}{cccccc} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \cancel{a_{11}} & \cdots & \cancel{a_{1j}} & \cdots & \cancel{a_{1m}} \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mm} \end{array} \right) \rightarrow j = 2, 3, \dots, m.$$

(6) EXEMPLU. Se determină o formă escalonată pe linii a matricei

$$A = \begin{pmatrix} 3 & -4 & -1 & 0 \\ 2 & -1 & 2 & 5 \\ 1 & 2 & 3 & 4 \\ 13 & -9 & 5 & 13 \\ 6 & -3 & 4 & 9 \end{pmatrix}$$

Aveam

$$A = \begin{pmatrix} 3 & -4 & -1 & 0 \\ 2 & -1 & 2 & 5 \\ 1 & 2 & 3 & 4 \\ 13 & -9 & 5 & 13 \\ 6 & -3 & 4 & 9 \end{pmatrix} \xrightarrow{\begin{array}{l} L_2 = 3L_2 - 2L_1 \\ L_3 = 3L_3 - 1L_1 \\ L_4 = 3L_4 - 13L_1 \\ L_5 = 3L_5 - 6L_1 \end{array}} \begin{pmatrix} 3 & -4 & -1 & 0 \\ 0 & 15 & 8 & 15 \\ 0 & 10 & 10 & 12 \\ 0 & 25 & 28 & 39 \\ 0 & 15 & 18 & 27 \end{pmatrix} \xrightarrow{\begin{array}{l} L_3 = 5L_3 - 10L_2 \\ L_4 = 5L_4 - 25L_2 \\ L_5 = 5L_5 - 15L_2 \end{array}} \begin{pmatrix} 3 & -4 & -1 & 0 \\ 0 & 5 & 8 & 15 \\ 0 & 0 & 130 & -9 \\ 0 & 0 & -60 & 18 \\ 0 & 0 & -30 & 90 \end{pmatrix}$$

$$\xrightarrow{\begin{pmatrix} 1 & 3 & -4 & -1 & 0 \\ 0 & 15 & 8 & 15 & \\ 0 & 0 & 130 & -90 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \end{pmatrix}} \xrightarrow{\begin{pmatrix} 1 & 3 & -4 & -1 & 0 \\ 0 & 15 & 8 & 15 & \\ 0 & 0 & 1 & 3 & \\ 0 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 0 & \end{pmatrix}} = A'$$

Să nu uităm că $\text{rglin}(A) = \text{rglin}(A')$. Mai mult, aveam proprietatea următoare.

(7) PROP. Linile nemulte ale unei forme extinse A' a matricei $A \in M_{m,n}(K)$ sunt vectori liniar indep. din K^n . În particular, linile nemulte ale matr. A' formează o bază pt. $\text{rglin}(A)$, prin urmare $\dim_K \text{rglin}(A) = n$, dim. liniar nemulte din A' .

Dem. Fie A' date de (2) și fie $\alpha_1 L'_1 + \dots + \alpha_r L'_r = 0$. Atunci,

$$(\alpha_1 a'_{11}, \dots, \alpha_1 a'_{1j_1} + \alpha_2 a'_{2j_2}, \dots) = (0, \dots, 0, \dots),$$

dе unde $\alpha_1 a'_{11} = 0$. Cum $a'_{11} \neq 0$ rezultă $\alpha_1 = 0$. Mai departe, $\alpha_1 a'_{1j_1} + \alpha_2 a'_{2j_2} = 0 \Rightarrow \alpha_2 = 0$, etc.

Un vector $v \in K^n$ se află în subspațiul $L(v_1, \dots, v_m)$, $v_i \in K^n$ dacă există în sisteme $\alpha_1, \dots, \alpha_m \in K$, s.t.

$$v = \alpha_1 v_1 + \dots + \alpha_m v_m$$

Ac. însăcum să decidă dacă un sistem de n ec. liniare cu necun-

$\alpha_1, \dots, \alpha_m$ este compatibil. Propoz. următoare ne oferă o metodă simplă de a decide dacă $v \in L(v_1, \dots, v_m)$,

(8) PROP. (Testul de apartenență). Fie v_1, \dots, v_m și v vectori din S.v. K^n și

$L_1 = v_1, \dots, L_m = v_m$, $L = \mathcal{L}$ linile matricei

$$A = \begin{pmatrix} l_1 \\ \vdots \\ l_m \\ L \end{pmatrix} \in M_{m+1, m}(k)$$

Astăzi, $v \in \mathcal{L}(v_1, \dots, v_m) \Leftrightarrow$ există un sir de op. elementare pe linii asupra matricei A care să transforme pe A într-o matrice A' în care linia L s-a devenit o linie nulă, adică A' este de formă

$$A' = \begin{pmatrix} l'_1 \\ \vdots \\ l'_m \\ 0 \end{pmatrix}$$

(fără a măsura generalitatea s-a presupus că op. elementare nu interzică schimbarea ultime linie)

Dem. \Rightarrow Dacă $v \in \mathcal{L}(v_1, \dots, v_m)$, at. există $\lambda_1, \dots, \lambda_m \in K$ s.ă. $v = \sum_{i=1}^m \lambda_i v_i$

Coresponditor, avem matricea A avem $L = \lambda_1 L_1 + \dots + \lambda_m L_m$. Succesivenele operații

$$A = \begin{pmatrix} l_1 \\ \vdots \\ l_m \\ L \end{pmatrix} \rightarrow \begin{pmatrix} l'_1 \\ \vdots \\ l'_m \\ L - \lambda_1 l_1 - \dots - \lambda_m l_m \end{pmatrix} \rightarrow \dots \rightarrow \begin{pmatrix} l'_1 \\ \vdots \\ l'_m \\ 0 \end{pmatrix}$$

conduc la o matrice în care linia L se transformă în linie nulă.

\Rightarrow Pres. că matricea A s-a transformat într-o matrice cu ultima linie nulă. Să observăm că fiecare op. elem. pe linii transformă pe A într-o matrice în care fiecare linie este o comb. liniară a liniei matricei A.

De exemplu, interzimbarea liniei L_i și L_j înseamnă că linia L_i este înlocuită cu comb. liniară $0 \cdot L_1 + \dots + 1 \cdot L_j + \dots + 0 \cdot L_m$; linia L_j este înlocuită cu comb. liniară $0 \cdot L_1 + \dots + 1 \cdot L_i + \dots + 0 \cdot L_m$. Cu scădere precizată, în final, linia L devine $L + \lambda_1 L_1 + \dots + \lambda_m L_m = 0$.

(9) EXEMPLU. Se decidem dacă $v = (10, 7, 0, 3) \in \mathcal{L}(v_1, v_2, v_3)$, unde $v_1 = (1, 2, -1, 4)$, $v_2 = (-2, 1, 0, 3)$, $v_3 = (3, 2, 1, -1)$. În ceea ce urmărește, vom evidenția scrierile lui A ca o comb. liniară a vectorilor v_1, v_2, v_3 . Avem:

$$\left(\begin{array}{c} l_1 \\ l_2 \\ l_3 \\ l_4 \\ L \end{array} \right) = \left(\begin{array}{cccc} 1 & 2 & -1 & 4 \\ -2 & 1 & 0 & 3 \\ 3 & 2 & 1 & -1 \\ 10 & 7 & 0 & 3 \end{array} \right) \xrightarrow{\begin{array}{l} l'_1 = l_1 \\ l'_2 = l_2 + 2l_1 \\ l'_3 = l_3 - 3l_1 \\ l'_4 = l_4 - 10l_1 \end{array}} \left(\begin{array}{cccc} 1 & 2 & -1 & 4 \\ 0 & 5 & -2 & 11 \\ 0 & -4 & 4 & -13 \\ 0 & -13 & 10 & -37 \end{array} \right) \xrightarrow{\begin{array}{l} l''_1 = l'_1 \\ l''_2 = l'_2 \\ l''_3 = 5l'_3 + 4l'_2 \\ l''_4 = 5l'_4 + 13l'_2 \end{array}} \left(\begin{array}{cccc} 1 & 2 & -1 & 4 \\ 0 & 15 & -2 & 11 \\ 0 & 0 & 12 & -21 \\ 0 & 0 & 24 & -42 \end{array} \right) \rightarrow$$

L1 - 6/9

$$\begin{array}{l} L_1''' = L_1'' \\ L_2''' = L_2'' \\ L_3''' = L_3'' \\ L_4''' = 12L_4 - 24L_3 \end{array} \rightarrow \begin{pmatrix} 1 & 2 & -1 & 4 \\ 0 & 5 & -2 & 11 \\ 0 & 0 & 12 & -21 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

, deci $\mathcal{J} \in \mathcal{L}(v_1, v_2, v_3)$. Pe de altă parte,

"reconstituind drumul" care a dus la linia ultimă egală cu zero, avem $0 = L_4''' = 12L_4 - 24L_3 = 12(5L_4 + 13L_2) - 24(5L_3 + 4L_2)$

$$= 60L_4 - 120L_3 + 60L_2$$

$$= 60(L_4 - 2L_3) - 120(L_3 - 3L_1) + 60(L_2 + 2L_1)$$

După simplificare cu 60 obținem

$$0 = L_4 - 10L_1 - 2(L_3 - 3L_1) + (L_2 + 2L_1)$$

$$= L_4 - 2L_1 + L_2 - 2L_3, \text{ și } L_4 = 2L_1 - L_2 + 2L_3.$$

(10) PROP. Linile matricii A care sunt transformate în linile rezultante ale unei forme escalonate a lui A formează o bază pentru $\text{rglin}(A)$.

Dem. Fie $A = \begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix}$ și $A' = \begin{pmatrix} L'_1 \\ \vdots \\ L'_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ o formă escalonată a lui A.

Pt. că $\text{rglin}(A) = \text{rglin}(A')$ rezultă că $\dim_{\mathbb{K}} \text{rglin}(A) = r$. Deoarece linia L_i s-a devenit linie nulă, avem:

$$L_i = \lambda_1 L_1 + \dots + \lambda_{i-1} L_{i-1} + \lambda_{i+1} L_{i+1} + \dots + \lambda_m L_m,$$

deci $\text{rglin}(A) = \mathcal{L}(L_1, \dots, L_{i-1}, L_{i+1}, \dots, L_m)$ și linia L_i poate fi exclusă dintr-o generatorie a lui $\text{rglin}(A)$. În acest fel, după $m-r$ pasi, obținem

$\text{rglin}(A) = \mathcal{L}(L_1, \dots, L_r)$. Linile L_1, \dots, L_r sunt r generatoare auto-nr. și tot de dimensiunea r $\Rightarrow B = \{L_1, \dots, L_r\}$ formează o bază a lui $\text{rglin}(A)$. ■

(11) APLICATIE. Să determinăm nr $r = \dim_{\mathbb{K}} \text{rglin}(A)$ și o bază alcătuită din r linii ale matricei

$$A = \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 1 & 4 & -3 & 4 & 2 \\ 2 & 3 & -1 & -2 & 9 \\ 1 & 3 & 0 & 2 & 1 \\ 1 & 5 & -6 & 6 & 3 \\ 2 & 5 & 3 & 2 & 1 \end{pmatrix}$$

Pentru a putea identifica linile care formează o bază vom evalua matricea A monitorizând inter schimbarea linilor.

$$A = \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \\ L_6 \end{pmatrix} = \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 1 & 4 & -3 & 4 & 2 \\ 2 & 3 & -1 & -2 & 3 \\ 1 & 3 & 0 & 2 & 1 \\ 1 & 5 & -6 & 6 & 3 \\ 2 & 5 & 3 & 2 & 1 \end{pmatrix} \xrightarrow{\text{RREF}} \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 0 & 1 & -1 & 2 & -1 \\ 0 & -3 & 3 & -6 & 3 \\ 0 & 0 & 2 & 0 & -2 \\ 0 & 2 & -4 & 4 & 0 \\ 0 & 1 & 7 & 2 & 5 \end{pmatrix} \xrightarrow{\text{RREF}} \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 0 & 1 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & -2 \\ 0 & 0 & -2 & 0 & 2 \\ 0 & 0 & 6 & 0 & -6 \end{pmatrix}$$

$$\xrightarrow{\text{RREF}} \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 0 & 1 & -1 & 2 & -1 \\ 0 & 0 & 2 & 0 & -2 \\ 0 & 0 & -2 & 0 & 2 \\ 0 & 0 & 6 & 0 & -6 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{RREF}} \begin{pmatrix} 1 & 3 & -2 & 2 & 3 \\ 0 & 1 & -1 & 2 & -1 \\ 0 & 0 & 2 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Deci, $B = \{L_1, L_2, L_4\}$ este o bază a lui $\text{rglin}(A)$ și $\dim_B \text{rglin}(A) = 3$.

Rangul unei matrice

Fie $A \in M_{m,n}(K)$ matricea dată de rel. (1), adică

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix}$$

Năște

$$A' = \begin{pmatrix} a_{11} & \dots & \dots & \dots & a_{1m} \\ 0 & \dots & 0 & a_{22} & \dots & \dots & a_{2m} \\ \dots & & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & a_{r2} & \dots & a_{rm} \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

o formă echivalentă a sa dată de rel. (2).

Până acum am văzut matricea sub formă

$$A = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_m \end{pmatrix}$$

unde L_i , $1 \leq i \leq m$, sunt vectorii din K^n . Coresponditor acestor situații am considerat $\text{rglin}(A) \subseteq K^m$.

Matricea a poartă și văzută și în formă $A = (c_1, \dots, c_n)$,

unde $c_j = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{mj} \end{pmatrix}$ este coloana j a lui A . Coresponditor, definim $\text{spcol}(A) = \mathcal{L}(c_1, \dots, c_n)$

Subspațiul $\text{spcol}(A) \subseteq K^m$ s.m. spațiuobținut lui A .

(12). TEOR. $\dim_K \text{spcol}(A) = \dim_K \text{splin}(A)$. Valoare comună a celor două dimensiuni s.m. rangul matr. A și se not. $\text{rang}(A)$.

Dem. Cu reprezentările (1) și (2), fiecare linie a matr. A se scrie ca o comb. liniară a vec. bazi $B = \{l'_1, \dots, l'_r\}$ a lui $\text{splin}(A)$.

Astfel,

$$\begin{cases} l_1 = \lambda_{11} l'_1 + \dots + \lambda_{1r} l'_r \\ l_2 = \lambda_{21} l'_1 + \dots + \lambda_{2r} l'_r \\ \vdots \\ l_m = \lambda_{m1} l'_1 + \dots + \lambda_{mr} l'_r \end{cases}$$

Pe componente obținem rel.

$$\begin{cases} a_{1j} = \lambda_{11} a'_{1j} + \dots + \lambda_{1r} a'_{1j} \\ a_{2j} = \lambda_{21} a'_{2j} + \dots + \lambda_{2r} a'_{2j} \quad \rightarrow j = 1, 2, \dots, m. \\ \vdots \\ a_{mj} = \lambda_{m1} a'_{mj} + \dots + \lambda_{mr} a'_{mj} \end{cases}$$

Al doilea set de egalit. înseamnă rel. vectorială

$$c_j = a'_{1j} \begin{pmatrix} \lambda_{11} \\ \lambda_{21} \\ \vdots \\ \lambda_{m1} \end{pmatrix} + a'_{2j} \begin{pmatrix} \lambda_{12} \\ \lambda_{22} \\ \vdots \\ \lambda_{m2} \end{pmatrix} + \dots + a'_{rj} \begin{pmatrix} \lambda_{1r} \\ \lambda_{2r} \\ \vdots \\ \lambda_{mr} \end{pmatrix} \quad j = 1, \dots, n$$

care exprune ω vectorii $\begin{pmatrix} \lambda_{1i} \\ \lambda_{2i} \\ \vdots \\ \lambda_{mi} \end{pmatrix}$ sunt r generatori si $\text{spcol}(A)$.

Adică, $\dim_K \text{spcol}(A) \leq \dim_K \text{splin}(A)$. Se observă că în ineq. are loc pentru orice matrice cu elemente din corpul K . Cu obs. suplimentară $\omega \text{spcol}(A) = \text{splin}(A^t)$ avem simbol de ineq.

$$\text{spcol}(A) = \text{splin}(A^t) \leq \text{splin}(A) = \text{splin}((A^t)^t) \leq \text{splin}(A^t) = \text{spcol}(A)$$

d.e.i. $\text{spcol}(A) = \text{splin}(A)$. ■

(13) LEMĂ. Fie $A \in M_n(K)$. Astfel

$\det(A) \neq 0 \iff$ orice formă extinsă a lui A are toate elementele de pe diagonale principale nulle.

Dem. Exercițiu ■

(14) TEOR. Fie $A \in M_{m,n}(K)$. Atunci,

$\text{rang}(A)=r \Leftrightarrow$ există un minor nenul de ordinul r al lui A și toti minorii de ordin $>r$ sunt nuli.

Dem. Denum. se bazează pe proprietățile determinantelor; suntem, deci în general, B este o matrice patratică și B_1 este o matrice obținută din B printr-un singur oper. elementare pe linii, astfel că $|B_1| = \alpha |B|$, unde $\alpha \in K^*$.

Fie A și A' matricile date de rel. (1) și (2). Fără să micșorez generalitatea putem presupune că fiecare linie L_i din A' provine din linia L_i a lui A . În caz contrar, se procedează la o permutare a liniilor în sensul egalității $\text{rang}(A) = L(L_1, \dots, L_m) = L(L_{\sigma(1)}, \dots, L_{\sigma(m)}) \rightarrow \forall \sigma \in S_m$.

\Rightarrow Minorul M' al matricei A ,

$$M' = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ 0 & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{rr} \end{vmatrix} \neq 0 \Rightarrow M = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix} \neq 0$$

$$\text{deoarece } M' = \alpha \cdot M, \alpha \in K^*.$$

Acum, pres. că $\exists A_1$, o submatrice patratică de ordin $s > r$ a lui A cu minorul $|A_1| \neq 0$. Cf. Lemă 13 orice formă echivalentă a lui A_1 are toate elem. de pe diag. principală nerule. $\text{rang}(A) = \dim_K \text{spcl}(A) = \dim_K L(C_{\sigma(1)}, \dots, C_{\sigma(r)})$ unde $\sigma \in S_m$ și putem pres. că coloanele lui A_1 sunt primele s coloane ale lui A . Fie B_1 submatricea lui A_1 alcătuită din cele s liniile ale lui A care au dat liniile lui A_1 . Orice echivalentă a lui B_1 va da s liniile nerule, deci $\text{rang}(A) > r$, contrad. cu ipoteza.

\Leftarrow Dacă, prin absurd, $\text{rang}(A) = s > r$, atunci din orice formă echivalentă A' a lui A , avem

$$A' = \begin{pmatrix} L_1 \\ \vdots \\ L_p \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

se poate extrage un minor nenul de ordin $p > r$, contrad.

(15) COR. $\text{rang}(A) = \text{nr. maxim de liniile liniare indep.}$

= nr. maxim de liniile liniare indep.

= ordinul maxim pt. care există un minor nenul

Lecția 2

Reprezentări matriciale ale unei operec. liniare

Așa cum vectorii sunt s.v. V de dimensiune n sau, reprezentări în s.v. familiar K^n , reprezentări mediate de baze B a lui V prin corespondență $v \longleftrightarrow (v)_B$, tot astfel o operec. liniară între două sp. vect. de dimensiune finită poate fi reprezentată prin matrice, motiv pt. că aceste matrice săn. reprezintă reprezentări matriciale ale operec. liniare.

Adică, fie $T: V \rightarrow U$ o operec. liniară definită pe s.v. V de dimensiune n cu valori în s.v. U de dimensiune m pe corpul K . Fie $B = \{e_1, \dots, e_n\}$ o bază a lui V și $B' = \{f_1, \dots, f_m\}$ o bază a lui U pe corpul K . Fie $v \in V$ și

$$v = x_1 e_1 + \dots + x_n e_n$$

Scriem într-o comb. lin. a vect. cu scalari x_1, \dots, x_n unic determinată. Atunci $(v) = (x_1, \dots, x_n)$. Calculăm $T(v)$ și avem:

$$T(v) = x_1 T(e_1) + \dots + x_n T(e_n).$$

Fiecare $T(e_i) \in U$ se scrie, la rândul său, ca o comb. liniară a vect. barei B' :

$$\begin{cases} T(e_1) = t_{11} f_1 + t_{12} f_2 + \dots + t_{1m} f_m \\ T(e_2) = t_{21} f_1 + t_{22} f_2 + \dots + t_{2m} f_m \\ \vdots \\ T(e_n) = t_{n1} f_1 + t_{n2} f_2 + \dots + t_{nm} f_m \end{cases} \quad (1)$$

Atunci $T(v)$ are expresia

$$T(v) = x_1 (t_{11} f_1 + t_{12} f_2 + \dots + t_{1m} f_m) + x_2 (t_{21} f_1 + t_{22} f_2 + \dots + t_{2m} f_m) + \dots + x_n (t_{n1} f_1 + t_{n2} f_2 + \dots + t_{nm} f_m)$$

$$\begin{aligned} &= (t_{11} x_1 + t_{12} x_2 + \dots + t_{1m} x_n) f_1 \\ &+ (t_{21} x_1 + t_{22} x_2 + \dots + t_{2m} x_n) f_2 \\ &\vdots \\ &+ (t_{n1} x_1 + t_{n2} x_2 + \dots + t_{nm} x_n) f_m \end{aligned}$$

Rezultă că

$$(T(v))_{B'} = \begin{pmatrix} t_{11} x_1 + t_{12} x_2 + \dots + t_{1m} x_n \\ t_{21} x_1 + t_{22} x_2 + \dots + t_{2m} x_n \\ \vdots \\ t_{n1} x_1 + t_{n2} x_2 + \dots + t_{nm} x_n \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1m} \\ t_{21} & t_{22} & \dots & t_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$\text{Definim } (T)_{B,B'} := \begin{pmatrix} t_{11} & \dots & t_{1m} \\ \vdots & \ddots & \vdots \\ t_{m1} & \dots & t_{mm} \end{pmatrix} \rightarrow$$

at. ultima relație se scrie

$$(T(v))_{B'} = (T)_{B,B'} (v)_B. \quad (2)$$

Matricea $(T)_{B,B'}$, cunoscută ca matricea de reprezentare a matricelor a aplicației liniare T în raport cu bazele B, B' . Dacă $T: V \rightarrow V$ este un operator liniar și $B' = B$, atunci matricea $(T)_{B,B'}$ se scrie, mai simplu, $(T)_B$, iar rel (2) devine rel. matriceală

$$(T(v))_B = (T)_B (v)_B. \quad (3)$$

(1) APLICAȚIE Fie $T: \mathbb{R}^n \rightarrow \mathbb{R}^m$ aplicație liniară definită prin

$$T(x_1, x_2, \dots, x_m) = (a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m, a_{21}x_1 + a_{22}x_2 + \dots + a_{2m}x_m, \dots, a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mm}x_m) \quad (4)$$

unde $a_{ij} \in \mathbb{R}$. Dacă $B = \{e_1, \dots, e_n\}$ este baza standard a lui \mathbb{R}^n și

$B' = \{f_1, \dots, f_m\}$ este baza standard a lui \mathbb{R}^m , atunci rel (1) ne dă

$$T(e_1) = T(1, 0, \dots, 0) = (a_{11}, a_{21}, \dots, a_{m1}) = a_{11}f_1 + a_{21}f_2 + \dots + a_{m1}f_m,$$

$$T(e_2) = T(0, 1, 0, \dots, 0) = (a_{12}, a_{22}, \dots, a_{m2}) = a_{12}f_1 + a_{22}f_2 + \dots + a_{m2}f_m,$$

$$T(e_m) = T(0, 0, \dots, 0, 1) = (a_{1m}, a_{2m}, \dots, a_{mm}) = a_{1m}f_1 + a_{2m}f_2 + \dots + a_{mm}f_m,$$

două

$$(T)_{B,B'} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}$$

în general

Domeniul în raport cu baza standard a lui K^n vectorul $v = (x_1, \dots, x_p)$ coincide cu vectorul corespondent, cunoscut $v = (v)_B$, pentru aplicație liniară dată, rel (2) se scrie

$$T(x_1, \dots, x_p) = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \quad (5)$$

Coincidența $v = (v)_B$ cind B este baza standard a spațiului K^n face ca orice aplicație liniară $T: K^n \rightarrow K^m$ să aibă legătură corespondență de (4) sau, echivalent, de (5).

(2) OBS. Evidențierea reprezentării matricale nu are ca scop final matricea

$(T)_{B,B}$. Semnificatia rel. (2) este aceea ca matricea aplic. liniară
 $T: V \rightarrow U$ este reprezentată de aplicatia liniară $K^n \rightarrow K^m$ date prin
 $x = (x_1, \dots, x_n) \mapsto (T)_{B,B} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ (6)

Si, mai mult, proprietatile lui T sunt același cu proprietatile aplic. liniare. (6).

De exemplu, fie $V = \{v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \mid a, b, c, d \in \mathbb{K} \text{ și } a+c=b+d\}$.

Pe V considerăm operaționalul liniar \bar{T} dat prin

$$\bar{T}: \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mapsto \begin{pmatrix} 2x+y & -x+y+z \\ z-w & 3x-w \end{pmatrix}$$

Se verifică faptul că mulțimea de vectori $B = \{e_1, e_2, e_3\}$ este o bază a lui V peste \mathbb{R} , unde

$$e_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, e_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, e_3 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

deci $\dim_{\mathbb{R}} V = 3$. Scrim vector $v = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ca o comb. liniară a vect. bazăi B . Si obținem $v_B = (c, d-c, b-c) \in \mathbb{R}^3$. Apoi, să determinăm matricea $(T)_B$:

$$T(e_1) = T \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 0 & 2 \end{pmatrix} = 0 \cdot e_1 + 2 \cdot e_2 + 1 \cdot e_3,$$

$$T(e_2) = T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = (-1) \cdot e_1 + 3 \cdot e_2 + 0 \cdot e_3,$$

$$T(e_3) = T \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = 0 \cdot e_1 + 3 \cdot e_2 + 0 \cdot e_3.$$

Deci,

$$(T)_B = \begin{pmatrix} 0 & -1 & 0 \\ 2 & 3 & 3 \\ 1 & 0 & 0 \end{pmatrix}$$

Acum, T este reprezentat de aplicatia liniară $A: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, date prin

$$(x_1, x_2, x_3) \mapsto \begin{pmatrix} 0 & -1 & 0 \\ 2 & 3 & 3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -x_2 \\ 2x_1 + 3x_2 + 3x_3 \\ x_1 \end{pmatrix} \quad (7)$$

Ilustrăm cum se determină $T(v) = T \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ folosind corespondența (7).

Aveam $(v)_B = (z, w-z, y-z)$ și în (3) obținem

$$(T(v))_B = \begin{pmatrix} 0 & -1 & 0 \\ 2 & 3 & 3 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} z \\ w-z \\ y-z \end{pmatrix} = \begin{pmatrix} 3x-z \\ 3x-z \\ z \end{pmatrix},$$

deci

$$T(v) = (z-w) e_1 + (3x-z) e_2 + z e_3 = \begin{pmatrix} z-w & z-w \\ z-w & z-w \end{pmatrix} + \begin{pmatrix} 3x-z & 0 \\ 0 & 3x-z \end{pmatrix} + \begin{pmatrix} z & z \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 3x+2z-w & 2z-w \\ z-w & 3x-w \end{pmatrix} = \begin{pmatrix} 2x+y & 2z-w \\ z-w & 3x-w \end{pmatrix}, \text{ deoarece } z+w=y.$$

Concluzia studiului reprezentării matriciale este că cernetarea aplicațiilor liniare $T: K^m \rightarrow K^m$ date prin rel (4) sau (5) reprezintă o variantă excelentă pentru cernetarea altor liniare $V \rightarrow U$, unde V este un s.v. de dimensiune n și U este un s.v. de dimensiune m .

Imaginează și nucleul unei aplicații liniare

Amențim că pentru aplicația $T: V \rightarrow U$,

$$\text{Ker } T = \{v \in V \mid T(v) = 0\},$$

$$\text{Im } T = \{u \in U \mid \exists v \in V \text{ s.t. } u = T(v)\}.$$

Imaginează $\text{Im } T$ poate fi determinată folosind propoz. următoare.

(3) PROP. Fie V și U două K -sp. vecți și $T: V \rightarrow U$ o aplic. liniară.

Dacă $\{v_1, \dots, v_r\}$ este o mulțime de generatori a lui V , atunci $\{T(v_1), \dots, T(v_r)\}$ este o mulțime de generatori a lui $\text{Im } T$.

Dem. Este suficient să arătăm că orice $u \in \text{Im } T$ este o comb. liniară a vectorilor $T(v_1), \dots, T(v_r)$. Într-adevăr, fie $u \in \text{Im } T$. At., există $v \in V$ s.t. $u = T(v)$. Pe de altă parte, $v = d_1 v_1 + \dots + d_r v_r$, unde $d_i \in K$, $1 \leq i \leq r$. Iată că $u = T(v) = T(d_1 v_1 + \dots + d_r v_r) = d_1 T(v_1) + \dots + d_r T(v_r)$. ■

(4) COR. Dacă $T: K^m \rightarrow K^m$ este aplic. liniară date prin

$$T(x_1, \dots, x_n) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

atunci $\text{Im } T$ este generat de coloanele matricei $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$.

Dem. Fie $B = \{e_1, \dots, e_n\}$ bază standard a lui K^n . Atenție

$$T(e_j) = T((0, \dots, 0, 1, 0, \dots, 0)) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} = c_j. \blacksquare$$

(5) OBS. Cor. 4 permite determinarea unei baze și dimensiunii subspațiului $\text{Im } T$ explorând matricea A^t . În particular, $\dim(\text{Im } T) = \text{rang}(A)$. Tot aici, observăm că $\text{Ker } T$ este multimea/spațiul soluțiilor sist. omogen de m

ec. liniare cu n necunoscute,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0, \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0. \end{cases} \quad (8)$$

Din teorema dimensiunii, $\dim(\mathbb{K}^n) = \dim(\text{Im } T) + \dim(\text{Ker } T)$, obținem că dimensiunea sp. soluțiilor sist.(8) e egală cu $\dim(\text{Ker } T) = n - \text{rang}(A)$.

APLICATIE. Se dă aplicație $T: \mathbb{R}^4 \rightarrow \mathbb{R}^3$, $T(x_1, x_2, x_3, x_4) = [-2x_1 - x_2 + x_4, -x_2 + x_3, x_1 + x_2]$

- Așteți că T este aplicație liniară
- Aflați și bere dimens. lui $\text{Im } T$
- Aflați $\dim_{\mathbb{R}}(\text{Ker } T)$.

Răspuns a) Execuție.

$$b) T(x_1, x_2, x_3, x_4) = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$\text{Im } T = \mathcal{L}(c_1, c_2, c_3, c_4) = \text{span}(A^t).$$

$$A^t = \begin{pmatrix} 2 & 0 & 1 \\ -1 & -1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Am obținut $\dim_{\mathbb{R}} \text{Im } T = 3$, și bere găsim $B = \{(2, 0, 1), (0, -2, 1), (0, 0, 1)\}$.

In definitie, $\text{Im } T = \mathbb{R}^3$.

$$c) \dim(\text{Ker } T) = \dim(\mathbb{R}^4) - \dim(\text{Im } T) = 4 - 3 = 1.$$

Sisteme de ecuații liniare

Forma generală a unui sistem de m ecuații liniare cu n necunoscute cu coeficienți numai în inel R este

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m, \end{cases} \quad (1)$$

Dacă $A = (a_{ij})$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ și $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, atunci (1) se scrie sub forma

$$Ax = b. \quad (2)$$

De asemenea, dacă $A = (c_1, \dots, c_n)$, unde c_j este coloana j a matricei A , atunci (1) se poate scrie sub forma

$$x_1c_1 + x_2c_2 + \dots + x_nc_n = b. \quad (3)$$

i. Regula lui Cramer se aplică sistemelor (1) în care numărul ecuațiilor este egal cu numărul necunoscutelor (deci, $m = n$) și $|A|$ este element inversabil în inelul R. Mai precis, avem proprietatea următoare.

PROP. 1 (Cramer) Dacă în sistemul (1) $m = n$ și $|A|$ este inversabil în inelul R, atunci sistemul (1) este compatibil determinist cu soluție unică (x_1, \dots, x_n) dată de formulele

$$x_j = \Delta_j / |A|, \quad j = 1, 2, \dots, n.$$

unde Δ_j este determinantul obținut din $|A|$ prin înlocuirea coloanei j cu vectorul termenelor liberi $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$.

Dem. Din $Ax = b$ se obține $x = A^{-1}b$, de unde unicitatea soluției $x = (x_1, \dots, x_n)$. Apoi, înmulțind ambele membri ai egalității $Ax = b$ cu matricea adjugată $A^* = (A_{ij}^*)^t$, unde A_{ij}^* este complementul algebric al elementului a_{ij} obținem $A^*Ax = A^*b$ sau $|A|x = A^*b$. Rezultă că

$$|A|x_j = A_{1j}^*b_1 + A_{2j}^*b_2 + \dots + A_{nj}^*b_n, \quad j = 1, 2, \dots, n.$$

relativ la care membrul stâng este dezvoltarea după col. j a determinanță obținută înlocuind în $|A|$ col. j cu coloana b .

2. Cazul sistemelor omogene. Multimea soluțiilor S a sist. omogen

$$a_{11}x_1 + \dots + a_{1n}x_n = 0 \quad (4)$$

$$a_{m1}x_1 + \dots + a_{mn}x_n = 0$$

cu coeficienți într-un corp comutativ K este un subspațiu al S.V. K^n de unde este nuanță explicită

$$X \rightarrow Ax, K^n \rightarrow K^m,$$

notări A. Deci, $S = \text{Ker } A$. Dacă rang - defect even

$$\dim(K^m) = \dim(\text{Im } A) + \dim(\text{Ker } A) = \text{rang}(A) + \dim(S).$$

$$\dim_K S = n - \text{rang}(A).$$

Fie $r = \text{rang}(A)$. Esalonarea pe linii a matricei $A \in M_{m,n}(K)$ transformă sistemul (4) într-un sistem echivalent de forme

$$A'x = 0,$$

cum

$$A' = \begin{pmatrix} 1 & & & & & \\ a_{11}' & \ddots & \cdots & \cdots & \cdots & a_{1m}' \\ 0 & \cdots & a_{21}' & \cdots & \cdots & a_{2n}' \\ \vdots & & \vdots & \ddots & \ddots & \vdots \\ 0 & & 0 & \ddots & \ddots & a_{rr}' \\ 0 & \cdots & 0 & \cdots & \ddots & 0 \\ \vdots & & \vdots & & & \vdots \\ 0 & & 0 & \cdots & & 0 \end{pmatrix}$$

După o reindexare a necunoscutelor putem presupune că A' este o matrice de forme

$$A' = \begin{pmatrix} a_{11}' & \cdots & \cdots & \cdots & a_{1m}' \\ 0 & a_{22}' & \cdots & \cdots & a_{2n}' \\ \vdots & 0 & \ddots & a_{rr}' & \cdots & a_{rn}' \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

cu $a_{ii}' \neq 0$, $i=1, 2, \dots, r$. Sistemul dat este echivalent cu sist. alcătuit numai din ec. 1, 2, ..., r. Adică, sist (4) este echivalent cu

$$\begin{pmatrix} a_{11}' & \cdots & \cdots & \cdots & a_{1m}' \\ a_{22}' & \cdots & \cdots & \cdots & a_{2n}' \\ 0 & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{rr}' & \cdots & a_{rn}' & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad (5)$$

cum

$$x_1 c'_1 + \dots + x_r c'_r + x_{r+1} c'_{r+1} + \dots + x_m c'_m = 0$$

sau, adică,

$$(c'_1 \dots c'_r) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = -x_{r+1} c'_{r+1} - \dots - x_m c'_m.$$

Holton $Ax = (c'_1, \dots, c'_r)$. Să îl scriem

$$Ax \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = -x_{r+1} c'_{r+1} - \dots - x_n c'_n \quad (6)$$

din

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = -x_{r+1} A^{-1} c'_{r+1} - \dots - x_n A^{-1} c'_n \quad (7)$$

In rel. (7) punem $x_{r+1} = 1, x_{r+2} = 0, \dots, x_n = 0$ și obținem

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = -A^{-1} c'_{r+1}$$

respectiv soluție săt (4),

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} -A^{-1} c'_{r+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Apoi, în (6) punem $x_{r+1} = 0, x_{r+2} = 1, x_{r+3} = 0, \dots, x_n = 0$ și
obținem

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} A^{-1} c'_{r+2} \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

La pasul $n-r$ obținem soluție

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} A^{-1} c'_n \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Care sunt soluții:

$$\begin{pmatrix} -A^{-1} c'_{r+1} \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -A^{-1} c'_{r+2} \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} A^{-1} c'_n \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

sunt $n-r$ vec. liniar independenti, deci formează baza lui S .

In definitie,

$$S = \left\{ \alpha_{r+1} \begin{pmatrix} -A_r^T C_{r+1}' \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \alpha_{r+2} \begin{pmatrix} -A_r^T C_{r+2}' \\ 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \dots + \alpha_{n-r} \begin{pmatrix} -A_r^T C_n' \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \mid \alpha_i \in K \right\} \quad (8)$$

Practic, rezolvarea sist. omogen (4) poate fi realizata in două moduri, și anume:

2) Considerand nec. x_{r+1}, \dots, x_n drept parametri, respectiv

$$x_{r+1} = \alpha_1, \dots, x_n = \alpha_{n-r}, \text{ rezolvem sist (6)}$$

$$Ax \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = -\alpha_1 C_{r+1}' - \dots - \alpha_{n-r} C_n'$$

folosind regula lui Cramer pentru necunoscutele x_1, \dots, x_r .

1) In sist. (5) dam succesiiv val. 1 unor din nec. x_{r+1}, \dots, x_n și cibaltele valenze 0, apoi rezolvem sist (5), obtinând vectorul soluției liniar indep. din (8).

EXERCITIU.

$$\begin{cases} x - 2y + 2z = 0 \\ 2x + y - 2z = 0 \\ 3x + 4y - 6z = 0 \\ 3x - 11y + 12z = 0. \end{cases}$$

OBS. Nec. x_1, \dots, x_r ai căror coef. sunt pivoti în forme eronate A^T s.n. nec. principale, iar celelalte care sunt parametri s.n. nec. secundare.

3. Cazul general. Ne ocupăm de sistemul (1) în cazul $R = K = \omega_{np}$. Prima problemă este de a stabili dacă sistemul este compatibil. Echivalența matricei (A, b) , numită matrice extinsă a sistemului și reindexarea necunoscătorilor conduce la sistemul

$$\begin{pmatrix} a_{11}' & \dots & a_{1m}' \\ 0 & a_{22}' & \dots & a_{2m}' \\ \vdots & \vdots & \ddots & a_{rr}' \dots a_{rm}' \\ 0 & 0 & \dots & 0 & \dots & a_{rn}' \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & & \dots & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \\ b_{r+1} \\ \vdots \\ b_m \end{pmatrix} \quad (3)$$

Se vede că cond. necesară pentru ca sist (3) să fie compatibil este ca toți $b_{r+1}, \dots, b_m = 0$, ceea ce înseamnă $\text{rg}(A, b) = \text{rg}(A)$.

Invers, dacă $\text{rang}(A, b) = \text{rang}(A)$, atunci sistemul săt (1) are forma

$$x_1c_1 + \dots + x_nc_n = b$$

rezultă că vectorul coloană b este o comb. liniară a coloanelor matricei A , deci $b \in \text{spol}(A)$. Astfel, am dem. următorul rezultat.

TEOR. Dacă nec. și suf. pentru că sist (1) să fie compatibil este că $\text{rang}(A, b) = \text{rang}(A)$. ■

Dacă sist (1) este compatibil, atunci este echiv. cu un sist. de forme

$$\begin{pmatrix} a_{11} & \dots & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{rr} & \vdots & a_{rn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \\ \vdots \\ b_n \end{pmatrix} \quad (10)$$

Privindu-l sub forma (10) sau (11), adică,

$$Ax \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = b - x_{r+1}c_{r+1} - \dots - x_nc_n \quad (11)$$

avem următoarea:

TEOR. Sol. generală a sist. compatibil (1) este suma dintre o sol. particulară a sist. și sol. generală a sistemului omogen asociat (4).

Dem. Fie U sol. generală a sist. (1) și fie $u_0 \in U$. At. $Au_0 = b$ și dacă $s \in S$, at. $As = 0$, apoi $A(u_0 + s) = b$, deci $u_0 + s \in U$. Astfel, $U + S \subseteq U$. Acum, fie $v \in U$ o sol. particulară. Avem $Av = b$. Obs. că $v = u_0 + (v - u_0)$, și că $A(v - u_0) = Av - Au_0 = b - b = 0$; deci, $v - u_0 \in S$. În definitie, $U \subseteq u_0 + S$, de unde $U = u_0 + S$. ■

O sol. particulară a sist (1) se poate obține rezolvând (11) pentru $x_{r+1} = \dots = x_n = 0$. Altfel, se rezolvă prin să se rezolve sist

$$\left\{ \begin{array}{l} Ax \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = b - \alpha_1 c_{r+1} - \dots - \alpha_n c_n, \\ x_{r+1} = \alpha_1, \\ x_n = \alpha_n, \end{array} \right. \quad \alpha_i \in K.$$

② Variante de Tvr. Kronecker-Capelli

Sist. echiv. cu (3), adică

$$x_1 c_1 + x_2 c_2 + \dots + x_n c_n = b.$$

Sist compatibil dacă $b \in L(c_1, \dots, c_n) \Leftrightarrow$ linia ultimă a unei forme echivalente a' mită

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \\ b \end{pmatrix} = \begin{pmatrix} A^t \\ b^t \end{pmatrix}$$

este linie nulă. În particular $\text{rang} \begin{pmatrix} A^t \\ b^t \end{pmatrix} = \text{rang} \begin{pmatrix} A^t \end{pmatrix} = \text{rang}(A)$ și

$$\text{rang} \begin{pmatrix} A^t \\ b^t \end{pmatrix} = \text{rang} \left(\begin{pmatrix} A^t \\ b^t \end{pmatrix}^t \right) = \text{rang}(A, b) \Rightarrow \text{rang}(A, b) = \text{rang}(A)$$

Dacă sist compatibil dacă ult. col. a unei forme echivalente a' mită

$$\begin{pmatrix} A^t \\ b^t \end{pmatrix}$$

este linie nulă.

Exemplu. Să se verifice dacă sistemul următor este compatibil.

$$\begin{cases} 5x + 3y - 11z = 13 \\ 4x - 5y + 4z = 18 \\ 3x - 13y + 19z = 22 \end{cases}$$

Sol.

Cu $A = \begin{pmatrix} 5 & 3 & -11 \\ 4 & -5 & 4 \\ 3 & -13 & 19 \end{pmatrix}$ și $b = \begin{pmatrix} 13 \\ 18 \\ 22 \end{pmatrix}$ săt. e compatibil dacă $\text{rang}(A,b) = \text{rang}(A)$.

Cele două ranguri se determină din elaborarea matricei (A,b) .

$$(A,b) = \begin{pmatrix} 5 & 3 & -11 & | & 13 \\ 4 & -5 & 4 & | & 18 \\ 3 & -13 & 19 & | & 22 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 3 & -11 & | & 13 \\ 0 & -37 & 64 & | & 38 \\ 0 & -74 & 128 & | & 71 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 3 & -11 & | & 13 \\ 0 & \cancel{-37} & 64 & | & 38 \\ 0 & 0 & 0 & | & -5 \end{pmatrix}$$

Audem $\text{rang}(A,b) = 3$ și $\text{rang}(A) = 2$, deci săt. incompatibil.

Exemplu. Să se verifice dacă săt. următor este compatibil și în ceață afirmație să se rezolve.

$$\begin{cases} 2x_1 + 3x_2 - x_3 + x_4 = 5 \\ x_1 - x_2 + 2x_3 - 2x_4 = -5 \\ 3x_1 + x_2 + 2x_3 - 2x_4 = -3 \\ x_2 - x_3 + x_4 = 3 \end{cases}$$

Sol. Înțeles, verificăm compatibilitatea:

$$(A,b) = \begin{pmatrix} 2 & 3 & -1 & 1 & | & 5 \\ 1 & -1 & 2 & -2 & | & -5 \\ 3 & 1 & 2 & -2 & | & -3 \\ 0 & 1 & -1 & 1 & | & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 & 2 & -2 & | & -5 \\ 2 & 3 & -1 & 1 & | & 5 \\ 3 & 1 & 2 & -2 & | & -3 \\ 0 & 1 & -1 & 1 & | & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 & 2 & -2 & | & -5 \\ 0 & 5 & -5 & 5 & | & 15 \\ 0 & 4 & -4 & 4 & | & 12 \\ 0 & 1 & -1 & 1 & | & 3 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & -1 & 2 & -2 & | & -5 \\ 0 & 1 & -1 & 1 & | & 3 \\ 0 & 1 & -1 & 1 & | & 3 \\ 0 & 1 & -1 & 1 & | & 3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -1 & 2 & -2 & | & -5 \\ 0 & 1 & -1 & 1 & | & 3 \\ 0 & 0 & 0 & 0 & | & 0 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix}$$

$$\text{rang}(A,b) = \text{rang}(A) \Rightarrow \text{săt. e compatibil}$$

Determinăm soluția generală: aceasta se obține rezolvând săt.

$$\begin{cases} x_1 - x_2 + 2x_3 - 2x_4 = -5 \\ x_2 - x_3 + x_4 = 3 \end{cases}, \quad (*)$$

cu nec. prime x_1, x_2 și nec. sec./parametru x_3, x_4 , astfel rezolvând săt.

$$\begin{cases} x_1 - x_2 = -5 - 2\alpha + 2\beta \\ x_2 = 3 + \alpha - \beta \\ x_3 = \alpha \\ x_4 = \beta \end{cases}$$

Se obține sol.

$$\begin{cases} x_1 = -2 - \alpha + \beta \\ x_2 = 3 + \alpha - \beta \\ x_3 = \alpha \\ x_4 = \beta \end{cases}, \text{ unde } \alpha, \beta \in \mathbb{R}$$

SAU

$$S = \{(-2 - \alpha + \beta, 3 + \alpha - \beta, \alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\}$$

$$= \{(-2, 3, 0, 0) + \alpha(-1, 1, 1, 0) + \beta(1, -1, 0, 1) \mid \alpha, \beta \in \mathbb{R}\},$$

unde

$u_0 = (-2, 3, 0, 0)$ este \Rightarrow sol. particulară a sistemului,

$\{\alpha(-1, 1, 1, 0) + \beta(1, -1, 0, 1) \mid \alpha, \beta \in \mathbb{R}\}$ este sol. generală a sist. omogen asociat

OBS. O sol. particulară a sist. neomogen se poate obține alegând $x_3 = x_4 = 0$,
 de unde $x_1 = -2$, $x_2 = 3$, respectiv sol. particulară $(x_1, x_2, x_3, x_4) = (-2, 3, 0, 0)$.

Vectorii generatori ai sist. omogen asociat pot fi determinați
 luând pt. nec. secundare $x_3 = 1, x_4 = 0$, de unde rezultă

$$\begin{cases} x_1 - x_2 = -2 \\ x_2 = 1 \end{cases}$$

furnizând vectorul $v(-1, 1, 1, 0)$. Apoi, luăm pt. nec. secundare $x_3 = 0, x_4 = 1$
 și obținem

$$\begin{cases} x_1 - x_2 = 2 \\ x_2 = 1 \end{cases}$$

Deci, un al doilea vector generator este $(1, -1, 0, 1)$ și mult. sol. sist.
 omogen este

$$\{\alpha(-1, 1, 1, 0) + \beta(1, -1, 0, 1) \mid \alpha, \beta \in \mathbb{R}\}.$$

Forme canonice pentru reprezentarea matricială a unui operator liniar

Introducere.

Fie $T: V \rightarrow V$ un op. liniar pe s.v. n-dimensional V pe corpul K .

Fie $B = \{e_1, \dots, e_n\}$ o bază a lui V/K . Legea de corespondență $v \mapsto T(v)$ este complet reprezentată de aplicația liniară $K^n \rightarrow K^n$, datează de legea

$$(v) \underset{B}{\mapsto} (T(v))_B \quad (1)$$

$$\text{în virtutea relației } (T(v))_B = (T_B(v))_B. \quad (2)$$

Matricea $(T)_B = (t_{ij})$ este datează de relațiile

$$\begin{cases} T(e_1) = t_{11}e_1 + t_{12}e_2 + \dots + t_{1n}e_n \\ T(e_2) = t_{21}e_1 + t_{22}e_2 + \dots + t_{2n}e_n \\ \vdots \\ T(e_n) = t_{n1}e_1 + t_{n2}e_2 + \dots + t_{nn}e_n \end{cases} \quad (3)$$

Avem în remarcă că din relația (3) rezultă $v = x_1e_1 + \dots + x_ne_n \Rightarrow T(v) = y_1e_1 + \dots + y_ne_n$, unde scalarii y_1, \dots, y_n se obțin din relația matricială

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad (4)$$

Vis-à-vis de aplicația liniară $T': K^n \rightarrow K^n$ datează de corespondență

$$(x_1, x_2, \dots, x_n) \mapsto (t_{11}x_1 + t_{12}x_2 + \dots + t_{1n}x_n, t_{21}x_1 + t_{22}x_2 + \dots + t_{2n}x_n, \dots, t_{n1}x_1 + t_{n2}x_2 + \dots + t_{nn}x_n) \quad (5)$$

indusă de T în s.v. K^n ,

(subliniem că pentru simplitate nu vom face descriere între relații $(x_1, \dots, x_n) \underset{\text{depozitiv}}{\sim} (x_1, \dots, x_n)^t$)

Facem obs. importantă că egalitatea (4) este relația matricială (2) pentru aplicația (5) atunci când baza lui K^n este baza standard/canonica adică $B_C = \{e_i = (1, 0, \dots, 0)\}, \dots, e_n = (0, 0, \dots, 0, 1)\}$. Deci, $(T)_B = (T')_{B_C}$.

Pentru acest motiv, studiul reprezentării matriciale a unui operator liniar pe un s.v. de dimensiune n poate fi efectuat pe operatori liniari pe K^n având legătură de corespondență (5), adică legătură

$$x \mapsto Ax, \quad (6)$$

unde $A \in M_n(K)$.

Cel puțin două probleme conduc la studiul reprezentării matriciale.

• Originea lor este legată de ceea ce: să fie identificat, dacă există, vectorii $\forall v \in V$ pentru care $T(v)$ este colinear cu vector v , adică $T(v) = \lambda v$, unde $\lambda \in K$.

\Rightarrow S.n. valoare proprie a aplicației T . Dacă dim $V = n$, și $\lambda_1, \dots, \lambda_n$ sunt n valori proprii distincte, atunci se demonstrează că există o bază B a lui V a.c.

$$(T)_B = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}. \quad (7)$$

Această reprezentare matricială a lui T este deosebit de avantajosă în decurțare, dacă $v = x_1 e_1 + \dots + x_n e_n$, atunci $T(v) = \lambda_1 x_1 e_1 + \dots + \lambda_n x_n e_n$.

Fie $\lambda \in K$ un scalar pt. care există $v \neq 0$ a.c. $T(v) = \lambda v$. Putem

$$V_\lambda = \{v \in V \mid T(v) = \lambda v\}$$

Astăzi V_λ este un subspațiu al lui V cu proprietatea

$$T(V_\lambda) \subseteq V_\lambda. \quad (8)$$

Legătura rel (7) și (8) studiul reprezentării matriciale este direcțional spre două probleme cu rezolvări conexe, anume:

(1) dacă există o bază B a s.v. V a.c. matricea $(T)_B$ să fie astăzi, dacă nu formează (7), măcar să formă cît mai aproape de (7).

Astfel de matrice s.n. forme canonice.

(2) identificarea subspațiilor $W \subseteq V$ care îndepl. condiția (8), adică $T(W) \subseteq W$. Astfel de subspații s.n. subspații T -invariante. Mai mult, poate fi: V = suma directă de subspații T -invariante, adică $V = W_1 \oplus W_2 \oplus \dots \oplus W_k$ cu $T(W_i) \subseteq W_i$, $i=1, 2, \dots, k$? ($V = W_1 \oplus \dots \oplus W_k$ înseamnă că $\forall v \in V$ se poate scrie $v = w_1 + \dots + w_k$, $w_i \in W_i$; să se arate că w_i sunt unice determinate de v).

1. Schimbarea bazei

Fie $B = \{e_1, \dots, e_n\}$ și $B' = \{f_1, \dots, f_m\}$ două baze ale s.v. n -dimensional V .

Fie $v \in V$. Pe de o parte,

$$v = x_1 e_1 + \dots + x_n e_n, \text{ deci } (v)_B = (x_1, \dots, x_n),$$

pe de altă parte,

$$v = y_1 f_1 + \dots + y_m f_m, \text{ prin urmare } (v)_{B'} = (y_1, \dots, y_m).$$

Fiecare vector f_i al bazei B' este o combinație liniară a vectorilor bazei B :

$$\begin{cases} f_1 = p_{11} e_1 + p_{12} e_2 + \dots + p_{1n} e_n \\ f_2 = p_{21} e_1 + p_{22} e_2 + \dots + p_{2n} e_n \\ \vdots \\ f_m = p_{m1} e_1 + p_{m2} e_2 + \dots + p_{mn} e_n \end{cases} \quad (9)$$

$$\begin{aligned}
 \text{Atunci, } v &= y_1 f_1 + y_2 f_2 + \cdots + y_m f_m \\
 &= y_1 (p_{11} e_1 + p_{12} e_2 + \cdots + p_{1n} e_n) \\
 &\quad + y_2 (p_{21} e_1 + p_{22} e_2 + \cdots + p_{2n} e_n) \\
 &\quad + \cdots \\
 &\quad + y_m (p_{m1} e_1 + p_{m2} e_2 + \cdots + p_{mn} e_n) \\
 &= (p_{11} y_1 + p_{12} y_2 + \cdots + p_{1n} y_n) e_1 \\
 &\quad + (p_{21} y_1 + p_{22} y_2 + \cdots + p_{2n} y_n) e_2 \\
 &\quad + \cdots \\
 &\quad + (p_{m1} y_1 + p_{m2} y_2 + \cdots + p_{mn} y_n) e_n
 \end{aligned}$$

Din unicitatea scrierii lui v ca o comb. liniară a vectorilor bazei B rezultă

$$\begin{cases} x_1 = p_{11} y_1 + p_{12} y_2 + \cdots + p_{1n} y_n \\ x_2 = p_{21} y_1 + p_{22} y_2 + \cdots + p_{2n} y_n \\ \vdots \\ x_n = p_{m1} y_1 + p_{m2} y_2 + \cdots + p_{mn} y_n \end{cases}$$

Dacă

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{mn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \quad (10)$$

ori

$$(v)_B = P_{B,B'} (v)_{B'}, \quad (10')$$

unde am notat $P_{B,B'} = (p_{ij})$

Matr. $P_{B,B'}$ s.m. matricea de trecere de la baza B la baza B' . Relația (10') s.m. schimbarea de coordonate; este trecerea de la coordonatele x_1, \dots, x_n la coordonatele y_1, \dots, y_n .

(1) PROP. Matricea $P_{B,B'}$ este inversabilă cu inversa $P_{B',B}$.

Dem. Dacă $(v)_B = P_{B,B'} (v)_{B'}$, și $(v)_{B'} = P_{B',B} (v)_B$ obținem $(v)_B = P_{B,B'} \cdot P_{B',B} (v)_B$. Înlocuim succesiv pe v cu e_1 , deci $(e_1)_B = (1, 0, \dots, 0)$, cu e_2 , deci $(e_2)_B = (0, 1, 0, \dots, 0)$ etc. și obținem $P_{B,B'} \cdot P_{B',B} = I_m$. Similar, se obține $P_{B',B} \cdot P_{B,B'} = I_m$. ■

(2) PROP. Fie $B = \{e_1, \dots, e_n\}$ o bază a s.v. V peste K . Dacă matricea $P = (p_{ij}) \in M_m(K)$ este inversabilă, atunci vectorii f_1, \dots, f_m date prin

$$\begin{cases} f_1 = p_{11} e_1 + p_{12} e_2 + \cdots + p_{1n} e_n \\ f_2 = p_{21} e_1 + p_{22} e_2 + \cdots + p_{2n} e_n \\ \vdots \\ f_m = p_{m1} e_1 + p_{m2} e_2 + \cdots + p_{mn} e_n \end{cases} \quad (11)$$

formelor, de asemenea, o bază B' a lui V . Mai mult, $P = (P)_{B,B'}$.

Dem. Ind. Este rcp. nr. astăzi a f_1, \dots, f_n sunt n vectori liniari independenți în s.v. de dimensiune n . ■

(3) COR. Fie $v_1 = (v_{11}, \dots, v_{1n}), v_2 = (v_{21}, \dots, v_{2n}), \dots, v_n = (v_{n1}, \dots, v_{nn})$ vectori în s.v. K^n peste K . Dacă $\det(A) \neq 0$, unde $A = (a_{ij})$, atunci vect. v_1, \dots, v_n alcătuiesc o bază a lui K^n .

Dem. Fie $B = \{e_1, \dots, e_n\}$ baza standard a lui K^n . Atunci, relațiile $v_i = a_{i1}e_1 + a_{i2}e_2 + \dots + a_{in}e_n, 1 \leq i \leq n$, inscriindu-ne în relația (11) cu matricea $P = A^t$, ■

Matricea de trecere $P_{B,B'}$ permite să obținem o relație între reprezentările $(T)_{B'} \text{ și } (T)_B$, analogă rel. (10') dintre $(v)_{B'} \text{ și } (v)_B$.

(4) PROP. Fie $T: V \rightarrow V$ un op. K -liniar pe s.v. V de dimensiune n .

Fie B și B' două baze ale lui V și $P := P_{B,B'}$. Atunci

$$(T)_{B'} = P^{-1}(T)_B P. \quad (12)$$

Dem. Scriem rel. $(Tv)_{B'} = P(T(v))_B$, sub formă echivalentă

$$(T)_{B'}(v)_{B'} = P(T)(v)_{B'},$$

$$(T)_{B'}P(v)_{B'} = P(T)_{B'}(v)_{B'}$$

Dăm succesiiv lui v valoările f_1, \dots, f_n , unde $B' = \{f_1, \dots, f_n\}$, obținem rel. $(T)_{B'} P = P(T)_{B'}$.

(5) COR. Fie $A \in M_n(K)$ reprezentarea matricială a op. liniar $T: V \rightarrow V$ în raport cu o bază B a lui V . Atunci

$$\{P'AP \mid P \text{ inversabil}\}$$

este multimea tuturor reprezentărilor matriciale ale lui T .

Dem. Exercițiu. ■

2. Vectori proprii și valori proprii

Fie V un s.v. peste corpul K și $T: V \rightarrow V$ un op. liniar.

(6) DEF. Un scalar $\lambda \in K$ s.n. valoare proprie dacă există un vector nenul $v \in V$ a.t.

$$T(v) = \lambda v. \quad (13)$$

Dacă vector ce satisfac rel. (13) s.n. vector propriu corespunzător valoiei proprii λ .

(7) PROP. Multimea, notată V_λ sau $V(\lambda)$ date prin

$$V_\lambda = \{v \in V \mid T(v) = \lambda v\}$$

este un subspațiu al lui V , numit spațiu propriu al lui λ . Mai mult V_λ este un subspațiu T -invariant al lui V , adică $T(V_\lambda) \subseteq V_\lambda$.

Dem. Se verifică că V_λ este subspațiu. Apoi, fie $B_\lambda = \{w_1, \dots, w_k\}$ o bază a lui V_λ . Dacă $v \in V_\lambda$ se scrie $v = \alpha_1 w_1 + \dots + \alpha_k w_k$. Atunci,

$$T(v) = \alpha_1 \lambda w_1 + \dots + \alpha_k \lambda w_k \in V_\lambda.$$

(8) EXEMPLU. Fie $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $T(x,y) = (x+5y, 2x+3y)$. Din rel. $T(1,1) = 5(1,1)$ deduce că $\lambda = 5$ este o val. proprie a lui T . Obs. că $\dim_{\mathbb{R}} V_\lambda < 2$, și în alt fel $V_\lambda = \mathbb{R}^2$ și $T(x,y) = 5(x,y)$, $\forall (x,y) \in \mathbb{R}^2$; deci $T(1,0) = (1,2) \neq 5(1,0)$. În aceste condiții $V_\lambda = L((1,1)) = \{\alpha(1,1) \mid \alpha \in \mathbb{R}\} = \{(\alpha, \alpha) \mid \alpha \in \mathbb{R}\}$.

(9) PROP. Vectorii proprii corespunzător valoiei proprii distincte sunt liniar independenti. Mai presus, vectorii nenuli $v_1, \dots, v_m \in V$ corespunzător val. proprii distincte $\lambda_1, \dots, \lambda_m \in K$ sunt liniar independenți.

Dem (inducție după m). Dacă $m=1$, atunci $\{v_1\}$ este liniar independent. Pres. $m \geq 2$ și fie

$$a_1 v_1 + \dots + a_m v_m = 0, \text{ unde } a_i \in K. \quad (14)$$

Apliind T rel. precedente și obținem

$$a_1 \lambda_1 v_1 + \dots + a_m \lambda_m v_m = 0. \quad (15)$$

Multiplicând rel. (14) cu λ_m și scădem din (15) obținem

$$a_1 (\lambda_1 - \lambda_m) v_1 + \dots + a_{m-1} (\lambda_{m-1} - \lambda_m) v_{m-1} = 0.$$

Cu ipot. de inducție obținem $a_1 = \dots = a_{m-1} = 0$. Ca și consecință, din (14) rezultă $a_m \lambda_m = 0$, deci $a_m = 0$.

(10) EXEMPLU. În s.v. $V = C^{\infty}(\mathbb{R})$ considerăm op. liniar $T = \text{derivare}$, adică $T(f) = f'$, $\forall f \in C^{\infty}(\mathbb{R})$. Considerăm vectorii (funcții) $e^{a_1 x}, \dots, e^{a_m x}$, unde a_1, \dots, a_m sunt m nr. reale distințe. Din $T(e^{a_i x}) = a_i e^{a_i x}$ rezultă că $e^{a_1 x}, \dots, e^{a_m x}$ sunt m vectori proprii aparținând valorilor proprii distințe a_1, \dots, a_m . În consecință, $e^{a_1 x}, \dots, e^{a_m x}$ sunt m vectori lin. indep. din p.v. $C^{\infty}(\mathbb{R})$.

(11) OBS. Reciproca prop. 9 nu este, în general, adevărată. Adică, dacă v_1, \dots, v_m sunt vect. proprii (nembi) lin. indep., nu rezultă că aparțin la valori proprii distințe. De exemplu, fie $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$
 $T(x, y, z) = (x - 3y + 3z, 3x - 5y + 3z, 6x - 6y + 4z)$.
 $T(1, 1, 0) = (-2, -2, 0) = -2(1, 1, 0)$ și $T(1, 0, -1) = (-2, 0, 2) = -2(1, 0, -1)$. Vectorii $u = (1, 1, 0)$ și $v = (1, 0, -1)$ sunt doi vectori proprii lin. indep. aparținând aceluiu de valori proprii $\lambda = -2$.

3. Diagonalaizare

Dacă v_1, \dots, v_n sunt n vectori proprii lin. indep. ai op. liniar $T: V \rightarrow V$, unde $\dim_k V = n$, vectori proprii aparținând val. proprii $\lambda_1, \dots, \lambda_n \in K$, mai neapărat distințe, atunci $B = \{v_1, \dots, v_n\}$ este o bază a lui V și din rel.

$$T(v_1) = \lambda_1 v_1 + 0v_2 + \dots + 0v_n$$

$$T(v_2) = 0v_1 + \lambda_2 v_2 + \dots + 0v_n$$

$$T(v_n) = 0v_1 + 0v_2 + \dots + \lambda_n v_n$$

rezultă că matricea lui T în bază B este

$$(T)_B = \begin{pmatrix} \lambda_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \lambda_n \end{pmatrix} \quad (16)$$

adică, $(T)_B$ este o matrice diagonală. Invers, dacă B este o bază a lui V în raport cu care matr. $(T)_B$ este diagonală, atunci B este alcătuit din vectori proprii ai lui T . Am dem. teorema următoare.

(12) TEOR. Fie $T: V \rightarrow V$ un op. liniar pe s.v. m-dimensional V .

T are o reprezentare matricială diagonală $\Leftrightarrow V$ are o bază B alcătuită din vectori proprii. În acest caz, elementele diagonalei matricei $(T)_B$ sunt valoarea proprie corespunzătoare și se spune că T este diagonalizabil.

(13) COR. Fie $A \in M_n(K)$ o reprezentare matricială a op. liniar $T: V \rightarrow V$.
Opér. T este diagonalizabil $\Leftrightarrow \exists P \in M_n(K)$ o matrice inversabilă a.t. $P^{-1}AP$ este o matrice diagonală.

Dem. Deoarece A este o reprezentare matricială a lui T , atunci cf. Cor. 5, $M(T) = \{P^{-1}AP \mid P \text{ inversabil}\}$ este multimea tuturor reprezentărilor matriciale ale lui T . Prin urmare, T este diagonalizabil d.s.m.d. există o matrice $P \in U(M_n(K))$ a.t. $P^{-1}AP$ este diagonală. ■

4. Determinarea valoarelor proprii

Folosind reprezentarea matricială, condiție ca $\lambda \in K$ să fie o valoare proprie a lui $T: V \rightarrow V$ poate fi exprimată prin urmatorul și de condiții echivalente via o bază B a lui V :

$$\left| \begin{array}{l} \exists v \neq 0 \text{ a.z.} \\ T(v) = \lambda v \end{array} \right\| \Leftrightarrow \left| \begin{array}{l} v \neq 0 \text{ a.z.} \\ (T(v))_B = \lambda (v)_B \end{array} \right\| \Leftrightarrow \left| \begin{array}{l} v \neq 0 \text{ a.z.} \\ (T_B(v))_B = \lambda (v)_B \end{array} \right\| \Leftrightarrow \left| \begin{array}{l} v \neq 0 \text{ a.z.} \\ ((\lambda I - (T)_B)(v))_B = 0 \end{array} \right\|$$

unde am notat cu I matricea unitate. Cu notările simplificării, $A := (T)_B$ și $x = (x_1, \dots, x_n) := (v)_B$, ultima cond. din simbol de echivalentă de mai sus afirmează că sistemul omogen de ec. liniare, scris sub formă matricială $(\lambda I - A)x = 0$,

are cel puțin o soluție nemănuire $x \in K^n$. Am dem. propozitivă.

(14) PROP. Fie $A \in M_n(K)$ o reprezentare matricială a opér. liniar $T: V \rightarrow V$.

Scaloul $\lambda \in K$ este o val. proprie a lui $T \Leftrightarrow \det(\lambda I - A) = 0$.

Altfel spus, λ este o valoare proprie $\Leftrightarrow \lambda$ e o sol. a ec. $\det(\lambda I - A) = 0$. ■

Acum, fie $A \in M_n(K)$ matricea lui T în baza B și fie $A_1 \in M_n(K)$ matricea lui T în baza B_1 a lui V . Atunci, $\det(\lambda I - A_1) = \det(\lambda I - A)$. Într-adevăr fie $A_1 = P^{-1}AP$. Avem $\det(\lambda I - A_1) = \det(P^{-1}A_1 P) = \det(P^{-1}((\lambda I)P - AP)) = \det(P^{-1}(\lambda I - A)P) = \det(P^{-1}) \cdot \det(\lambda I - A) \det(P) = \det(\lambda I - A)$.

$$\text{Egalitatea } \det(\lambda I - A) = \det(\lambda I - A_1)$$

este suportul defin. imunitare.

(15) DEF. Fie $A \in M_n(K)$ și reprezentare matricială a op. liniară $T: V \rightarrow V$.

Polynomiel

$$\Delta_T(\lambda) := \det(\lambda I - A)$$

S.n. polinomul caracteristic al lui T , iar ec. $D_T(\lambda) = 0$ ale cărei soluții sunt valori proprii ale lui T . S.n. ecuația caracteristică a lui T .

Orice matrice $A \in M_n(K)$ poate fi reprezentată ca reprezentanță matricială a unei op. liniare T definite pe un s.v. de dimensiune n . Într-adevăr, dacă $B = \{e_1, \dots, e_n\}$ este o bază a lui V , atunci op. $T: V \rightarrow V$ este prin

$$T(e_1) = e_{11}e_1 + e_{21}e_2 + \dots + e_{m1}e_m$$

$$T(\ell_2) = \alpha_{12} e_1 + \alpha_{22} e_2 + \dots + \alpha_{m2} e_m,$$

$$T(\ell_m) = \ell_{m1} e_1 + \ell_{m2} e_2 + \dots + \ell_{mn} e_n,$$

are $(T)_B = A$. Din acest motiv, multumile de vectori proprii și valori proprii se extind asupra matricei A , eventual privită ca op. liniar $A: K^n \rightarrow K^n$, dat prin $x \mapsto Ax$, unde $x = (x_1, \dots, x_n) \in K^n$. În definitiv, polinomul în λ

$$\Delta_A(\lambda) := \det(\lambda I - A)$$

s.n. polinomul caracteristic al matr. A , ic. $\Delta_A(\lambda) = 0$.

S.m. characteristic a mat. A i. a sol. i.e. $\Delta_A(\lambda) = 0$ s.m.

val. proprie a matricei A, non \Rightarrow sol. $x \neq 0$ sc. $(\lambda I - A)x = 0$ echivalent cu $Ax = \lambda x$ s.m. vector propriu. În fine, matr. A s.m. diagonalizabilă d.c.t. $\exists P \in U(M_n(k))$ s.t. $P^{-1}AP$ este matrice diagonală.

(16) EXEMPLU. Si scriem ec. caracteristică $\Delta_f(\lambda) = 0$ pt. op. liniar $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ det

$$\text{poww } T(x_1, x_2, x_3) = (2x_1 - x_2 + 5x_3, 7x_1 - 4x_3, 6x_1 + 5x_2).$$

Scriem pe $T(x_1, x_2, x_3)$ ca vector coloană și obținem

$$T(x_1, x_2, x_3) = \begin{pmatrix} 2x_1 - x_2 + 5x_3 \\ 7x_1 - 4x_3 \\ 6x_1 + 5x_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 5 \\ 7 & 0 & -4 \\ 6 & 5 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = Ax.$$

A este matricea lui T în baza standard a lui \mathbb{R}^3

In consequence, etc. correct. a limit exists

$$|\lambda I - A| = \left| \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} - \begin{pmatrix} 2 & -1 & 5 \\ 7 & 0 & -4 \\ 6 & 5 & 0 \end{pmatrix} \right| = \begin{vmatrix} \lambda-2 & 1 & -5 \\ -7 & \lambda & 4 \\ -6 & -5 & \lambda \end{vmatrix} = 0.$$

(17) OBS. Fie $T: K^n \rightarrow K^n$, $T(x) = Ax$ un op. liniar diagonalizabil. Atunci, $A = (T)_B$, unde B este baza standard a lui K^n .

Matricea P de trecere de la baza standard B la baza B' este data de vectorii proprii v_1, \dots, v_n corespunzănd val. propriei $\lambda_1, \dots, \lambda_n \in K$ și sunt drept obânci par să simboliceze vectorii v_1, v_2, \dots, v_n . Acesta, avem ce să vedem $v_1 = (p_{11}, p_{12}, \dots, p_{1n}) \rightarrow v_2 = (p_{21}, p_{22}, \dots, p_{2n}) \rightarrow \dots \rightarrow v_n = (p_{n1}, p_{n2}, \dots, p_{nn})$, astfel că formulele de trecere de la baza B la baza B' sunt

$$\begin{cases} v_1 = p_{11}e_1 + p_{12}e_2 + \dots + p_{1n}e_n \\ v_2 = p_{21}e_1 + p_{22}e_2 + \dots + p_{2n}e_n \\ \vdots \\ v_n = p_{n1}e_1 + p_{n2}e_2 + \dots + p_{nn}e_n \end{cases}$$

Atenție, că

$$P(v_1, v_2, \dots, v_n)$$

are loc egalitățile

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \quad (17)$$

de unde ambele membri ai egalității sunt $(T)_B$.

(18) APLICATIE. Se găsește valoile proprii și sp. propriei corespondente pentru matricea

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}. \quad \text{Deoarece } A \text{ este diagonalizabil se evident că matr. } P \text{ pt care } P^{-1}AP \text{ este diagonală.}$$

Soluție. T.c. există o liniă A astfel că $\begin{vmatrix} \lambda-1 & -4 \\ -2 & \lambda-3 \end{vmatrix} = 0$, adică $\lambda^2 - 4\lambda - 5 = (\lambda+1)(\lambda-5) = 0$.

Sunt doar val. propriei, anume $\lambda = -1$ și $\lambda = 5$.

Vectorii proprii ai val. propriei $\lambda_1 = -1$ sunt soluțiile ecuației:

$$A \begin{pmatrix} x \\ y \end{pmatrix} = (-1) \begin{pmatrix} x \\ y \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ -y \end{pmatrix} \Leftrightarrow \begin{cases} x+2y=0 \\ 2x+3y=0 \end{cases}$$

Mult. sl. / sp. propriei este $V_{\lambda_1} = \{\alpha(-2, 1) \mid \alpha \in \mathbb{R}\} = \{(2\alpha, \alpha) \mid \alpha \in \mathbb{R}\} = \mathcal{L}((-2, 1))$

Vectorii proprii ai val. propriei $\lambda_2 = 5$ sunt sl. ecuației:

$$A \begin{pmatrix} x \\ y \end{pmatrix} = 5 \begin{pmatrix} x \\ y \end{pmatrix} \Leftrightarrow x-y=0.$$

Deci, $V_{\lambda_2} = \{\alpha(1, 1) \mid \alpha \in \mathbb{R}\} = \mathcal{L}((1, 1))$.

Vectorii proprii $v_1 = (-2, 1)$ și $v_2 = (1, 1)$ formează o bazu B' a lui \mathbb{R}^2 în raport cu care

$$(T)_{B'} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 5 \end{pmatrix}.$$

Aici, $\begin{pmatrix} -1 & 0 \\ 0 & 5 \end{pmatrix} = P^{-1}AP$, unde $P = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$.

(19) OBS. O verificare a rel. (17) nu necesită calculul lui P^{-1} deoarece (17) este echivalent cu $AP = P \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$.

Forme canonice (continuare)

Am văzut că, via o bază B a s.v. n -dimensional V , determinarea valorilor proprii a op. liniar $T: V \rightarrow V$ devine o problemă matricială, prin echivalentă.

λ val. proprie $T \Leftrightarrow \lambda$ este sol. a ec. $\det(\lambda I - A) = 0$, unde $A = (T)_B$. Mai mult, determinarea vectorilor proprii apartinând valoiei proprii $\lambda \in K$ înseamnă rezolvarea sistemului de ec. liniare având forme matriciale:

$$(\lambda I - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0. \quad (1)$$

Dacă $(x_1, \dots, x_n) \in K^n$ este o soluție a ec. (1) și $B = \{e_1, \dots, e_n\}$, atunci vectorul propriu al valoiei proprii λ este $v = x_1 e_1 + \dots + x_n e_n$, pentru că $T(v) = \lambda v$ și $(T(v))_B = (T)_B(v)_B$ conduce, cu notările $A = (T)_B$ și $(x_1, \dots, x_n) = |v\rangle_B$, la ec. (1).

Pentru aceste motive, în continuare, problemele valorilor și vectorilor proprii o vom raporta la o matrice.

Asadar, fie $A \in M_n(K)$ și notăm $\Delta_A(\lambda) := \det(\lambda I - A)$ polinomul caracteristic al matricei A . Din expresie

$$\Delta_A(\lambda) = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{vmatrix}$$

obținem

$$\Delta_A(\lambda) = (\lambda - a_{11})(\lambda - a_{22}) \cdots (\lambda - a_{nn}) + \text{termeni cu cel mult } (n-2) \text{ factori de formă } \lambda - a_{ii}.$$

$$= \lambda^n - (a_{11} + a_{22} + \cdots + a_{nn}) \lambda^{n-1} + \text{termeni de grad mai mic în } \lambda$$

(1) TEOREMĂ (Hamilton-Cayley). Orice matrice patratică este un zero al polinomului său caracteristic.

Dem. Fie $A \in M_n(K)$ și fie $\Delta_A(\lambda) = \lambda^n + a_{n-1} \lambda^{n-1} + \cdots + a_1 \lambda + a_0$. Fie $B(\lambda)$ matricea adjunctă a lui $\lambda I - A$. Elementele lui $B(\lambda)$ sunt polinome în λ de gradul cel mult $n-1$. Atunci, fie

$$B(\lambda) = B_{n-1} \lambda^{n-1} + \cdots + B_1 \lambda + B_0, \quad \text{unde } B_i \in M_n(K).$$

Din relația

$$(\lambda I - A)B(\lambda) = [\lambda I - A]$$

se urmărește sub forma

$$(\lambda I - A)(B_{m-1}\lambda^{m-1} + B_{m-2}\lambda^{m-2} + \dots + B_1\lambda + B_0) = (\lambda^m + a_{m-1}\lambda^{m-1} + \dots + a_1\lambda + a_0) I$$

rezultă

$$B_{m-1} = I$$

$$B_{m-2} - AB_{m-1} = a_{m-1} I$$

$$B_{m-3} - AB_{m-2} = a_{m-2} I$$

$$B_0 - AB_1 = a_1 I$$

$$-AB_0 = a_0 I$$

Înmulțim relațiile precedente respectiv cu A^m , A^{m-1} , ..., A^2 , și adunăm rel. obținute. Rezultă

$$0 = A^m + a_{m-1}A^{m-1} + \dots + a_1A + a_0 I.$$

Matrice diagonalizabile. Operator diagonalizabil

Fie $A \in M_n(K)$. Dacă A este diagonalizabilă, atunci $\exists P \in U(M_n(K))$ s.t. $P^{-1}AP$ este o matrice diagonală de forma

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ 0 & & \lambda_m \end{pmatrix} \quad (2)$$

$\lambda_1, \dots, \lambda_m$ sunt valoare proprii (nu neapărat distinse) ale lui T .

Prin urmare,

$$\Delta_A(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_r)^{m_r}, \quad m_1 + \dots + m_r = n \quad (3)$$

Invers, descompunerea (3)-care înseamnă că toate valoile proprii ale lui A sunt în K -nu este o condiție suficientă pentru ca matricea A să fie diagonalizabilă sub forma (2), aşa cum rezultă din exemplul următor.

$$(2) \text{ EXEMPLU. Fie } A \in M_3(\mathbb{R}), \quad A = \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & -2 \end{pmatrix} \quad \text{Acum, } \Delta_A(\lambda) = (\lambda+2)^2(\lambda-4).$$

Pentru $\lambda = -2$, V_{-2} este mult. sol. ec. $Ax = -2x$ sau $(2I + A)x = 0$, unde $x = (x_1, x_2, x_3)$. Se obține: $\dim_{\mathbb{R}} V_{-2} = 1$ și o bază a spațiului propriu V_{-2} este $\{v_{-2} = (1, 1, 0)\}$.

$$V_{-2} = \mathcal{L}((1, 1, 0)) = \langle (1, 1, 0) \rangle = \{\alpha(1, 1, 0) \mid \alpha \in \mathbb{R}\}.$$

Acum să aflăm sp. propriu V_λ și să vedem că ea pt. val. proprie $\lambda = 4$.

Ec. $(\lambda I - A)x = 0$ înv. sistemul omogen

$$\begin{pmatrix} 7 & -1 & 1 \\ 7 & -1 & 1 \\ 6 & -6 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} 7x_1 - x_2 + x_3 = 0 \\ x_1 = 0 \end{cases}$$

Atunci, $V_\lambda = \{(0, \alpha, \alpha) \mid \alpha \in \mathbb{R}\} = \{\alpha(0, 1, 1) \mid \alpha \in \mathbb{R}\} = \langle (0, 1, 1) \rangle$.

Deci $\dim_{\mathbb{R}} V_\lambda = 1$ cu o bază alcătuită din vect $v_2 = (0, 1, 1)$.

Hu există deci doi vectori proprii liniali independenți, avemne v_1, v_2 , care nu pot forma o bază a lui \mathbb{R}^3 . Conform Teor 12/1 operatorul $x \mapsto Ax$ nu este diagonalizabil deci matricea A nu e diagonalizabilă.

(3) PROPR.: Fie $T: V \rightarrow V$ o transf. liniară în s.v. finit dimensional V , iar $\lambda_0 \in K$ o valoare proprie de multiplicitate m , adică

$$\Delta_T(\lambda) = (\lambda - \lambda_0)^m Q(\lambda), \quad Q(\lambda_0) \neq 0.$$

Atunci, $\dim_{\mathbb{K}} V_{\lambda_0} \leq m$.

Dem. Fie $\{v_1, \dots, v_s\}$ o bază a lui V_{λ_0} . Completăm bază $\{v_1, \dots, v_s\}$ printr-o bază $B = \{v_1, \dots, v_s, w_{s+1}, \dots, w_m\}$ a lui V . Din relațile

$$T(v_i) = \lambda_0 v_i$$

:

$$T(v_s) = \lambda_0 v_s$$

$$T(w_{s+1}) = t_{1,s+1} v_1 + \dots + t_{s,s+1} v_s + t_{s+1,s+1} w_{s+1} + \dots + t_{m,s+1} w_m$$

$$T(w_m) = t_{1,m} v_1 + \dots + t_{s,m} v_s + t_{s+1,m} w_{s+1} + \dots + t_{m,m} w_m$$

rezultă că

$$(T)_B = \begin{pmatrix} \lambda_0 & 0 & t_{1,s+1} & \dots & t_{1,m} \\ 0 & \lambda_0 & t_{2,s+1} & \dots & t_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & t_{s,s+1} & \dots & t_{s,m} \end{pmatrix} \quad (4)$$

Din (4) rezultă că

$$\Delta_T(\lambda) = (\lambda - \lambda_0)^s Q_1(\lambda), \quad \text{deci } s \leq m. \blacksquare$$

(4) PROP. (Formă alternativă a Prop. 3). Fie $A \in M_n(K)$ și $\lambda_0 \in K$ o valoare proprie de multiplicitate m a matricei A , adică

$$\Delta_A(\lambda) = (\lambda - \lambda_0)^m Q(\lambda), \quad Q(\lambda_0) \neq 0.$$

Atunci, $\dim_{K\lambda_0} V_{\lambda_0} \leq m$.

Ordinalul de multiplicitate al val. proprii $\lambda \in K$ s.n. multiplicitatea algebrică a lui λ , iar $\dim_{K\lambda} V_{\lambda}$ s.n. multiplicitatea geometrică a lui λ . Prop. 3 și Prop. 4 afirme că multiplicitatea geometrică a val. proprii $\lambda \leq$ multiplicitatea algebrică.

Teorema următoare clarifică pe dețin constituite în care un operator liniar este diagonalizabil, respectiv o matrice patratică este diagonalizabilă.

(5) TEOR. Fie $T : V \rightarrow V$ o transformare liniară a s.v. V de dimensiunea n și fie

$$\Delta_T(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_r)^{m_r}, \quad m_1 + \cdots + m_r = n$$

o descomp. a polinomului caracteristic în factori liniari peste K . U.A.E. :

(i) T este diagonalizabil;

(ii) $\dim_{K\lambda_i} V_{\lambda_i} = m_i$, $\forall i = 1, r$. Adică, pentru fiecare val. proprie $\lambda_i \in K$, nr. vectorilor proprii liniari independenți aparținării val. proprii λ_i egalează ordinalul de multiplicitate al lui λ_i .

Dem. (i) \rightarrow (ii). Dacă T este diagonalizabil și v_1, \dots, v_n sunt n vectori proprii liniari indep. ai lui T , atunci folosind Prop. 3, ei pot fi grupați în $\{v_1, \dots, v_{m_1}\} \subset V_{\lambda_1}, \{v_{m_1+1}, \dots, v_{m_1+m_2}\} \subset V_{\lambda_2}, \dots, \{v_{m_1+\dots+m_{r-1}+1}, \dots, v_{m_1+\dots+m_r}\} \subset V_{\lambda_r}$ și conform Prop. 3 avem $m_i \leq m_1, \dots, m_r \leq m_r$. Pe de altă parte, $m_1 + \dots + m_r = n$ devine T este diagonalizabil și din $n = m_1 + \dots + m_r \leq m_1 + \dots + m_r = n$ rezultă $m_i = m_i$ pentru toți $i = 1, r$.

(ii) \Rightarrow (i). Rezultă din Prop. 3 a lecției 3, cf. cărția vectorii proprii care aparțin la valori proprii diferențe sunt liniari indep. Mai exact, fie multimiile de vectori liniari indep. $\{v_{1,1}, \dots, v_{1,m_1}\} \subset V_{\lambda_1}, \dots, \{v_{r,1}, \dots, v_{r,m_r}\} \subset V_{\lambda_r}$ și fie $\alpha_{11}v_{1,1} + \dots + \alpha_{1m_1}v_{1,m_1} + \dots + \alpha_{r1}v_{r,1} + \dots + \alpha_{rm_r}v_{r,m_r} = 0$, (3)

cu $\alpha_{ij} \in K$.

Punem $w_1 = \alpha_{11}v_{1,1} + \dots + \alpha_{1m_1}v_{1,m_1}, \dots, w_r = \alpha_{r1}v_{r,1} + \dots + \alpha_{rm_r}v_{r,m_r}$.

$$\text{avem } w_1 + \dots + w_r = 0,$$

\Rightarrow rel. în care w_i este val. proprie a lui λ_i , $i=1, r$. Deci nu toți veci w_1, \dots, w_r sunt nuli, atunci însămătării sunt linear dependenți, în contrad. cu Prop. 9/L1. Astfel, $w_1 = \dots = w_r = 0$ și mai departe toți veci rel. (3) sunt nuli. ■

(6) COR. (Formă alternativă a Teor. 5). Pentru matricea $A \in M_n(K)$, U.A.E.:

(i) A este diagonalizabilă;

(ii) $\Delta_A(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_r)^{m_r}$, cu $m_1 + \dots + m_r = n$ și $\lambda_i \in K$, iar $\dim_{K\lambda_i} V_{\lambda_i} = m_i$, $\forall i = 1, r$.

(7) APLICATIE. Fie $A = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 5 & -6 \\ -4 & -4 & 10 \end{pmatrix} \in M_3(\mathbb{R})$.

(a) Afleati val. proprii și spațiile proprii corespunzătoare.

(b) Arătați că A este diagonalizabilă, scriind matricea $P \in U(M_3(\mathbb{R}))$ a.t. $P^{-1}AP$ este diagonală și scriind o formă diagonală a lui A .

Ind. $\lambda = 2$ este o rid. a ec. caracteristică a lui A .

(8) OBS. (O tehnică de a obține o matrice diagonalizabilă, cazul $n=3$)

$A \in M_3(\mathbb{R})$ diagonalizabilă dacă

(a) A are trei valori proprii reale diferite

(b) A are trei valori proprii reale $\lambda_1, \lambda_2, \lambda_3$, două egale, de ex. $\lambda_1 = \lambda_2$ și $\dim V_{\lambda_1} = 2$. În acest caz, sp. sol. sist. omogen $(A - \lambda_1 I)X = 0$ tb. se ește dimensiunea egală cu 2, deci tb. se poate scrie de forma

$$\begin{cases} ax + by + cz = 0, \\ mx + ny + nz = 0, \\ px + qy + rz = 0, \end{cases} \quad (*)$$

Pt. 9 săt. (x) este echiv cu

$$\begin{pmatrix} a & b & c \\ ma & mb & mc \\ pa & pb & pc \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

aleg λ_0 rid. dublă și aleg pe $\lambda_0 - A$ ca fiind

$$\begin{pmatrix} \lambda_0 - (\lambda_0 - a) & b & c \\ ma & \lambda_0 - (\lambda_0 - mb) & mc \\ pa & pb & \lambda_0 - (\lambda_0 - pc) \end{pmatrix} \cdot At \cdot A = \begin{pmatrix} \lambda_0 - a & -b & -c \\ -ma & \lambda_0 - mb & -mc \\ -pa & -pb & \lambda_0 - pc \end{pmatrix}$$

(9) PROP. Dacă $T: V \rightarrow V$ este un op. diagonalizabil cu valori proprii $\lambda_1, \dots, \lambda_r$ și spații proprii $V_{\lambda_1}, \dots, V_{\lambda_r}$, atunci subspacele $V_{\lambda_1}, \dots, V_{\lambda_r}$ ale lui V realizează o descompunere a lui V într-o sumă directă de subspace T -invariante. Mai presus,

$$V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_r}, \text{ cu } T(V_{\lambda_i}) \subseteq V_{\lambda_i}, i = 1, r$$

Egalitatea $V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_r}$ înseamnă că $V = V_{\lambda_1} + \dots + V_{\lambda_r}$ și $V_{\lambda_i} \cap (V_{\lambda_1} + \dots + V_{\lambda_{i-1}} + V_{\lambda_{i+1}} + \dots + V_{\lambda_r}) = \{0\}, \forall i$. Prințic, $\forall v \in V$ se scrie ca o sumă $v = v_1 + \dots + v_r$, cu $v_i \in V_{\lambda_i}$ unic determinată, și $T(v) = \sum_{i=1}^r T(v_i) = \sum_{i=1}^r \lambda_i v_i$.

Forma canonică triangulară

Fie $T: V \rightarrow V$ un op. liniar pe s.v. n-dimens V . Dacă T are n valori proprii în K și

$$\Delta_T(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_r)^{m_r}, m_1 + \dots + m_r = n,$$

dacă există cel puțin un sp. propriu V_{λ_i} , c.e. $\dim_K V_{\lambda_i} < m_i$, atunci cf. Teor. 5 op. T nu este diagonalizabil. Totuși, teoreme următoare ne asigură că T are o reprezentare matricială triangulară triangulară.

(10) TEOR. Fie $T: V \rightarrow V$ un op. liniar pe K -sp. vectorial n-dimens. V .

Există o reprezentare matricială a lui T printr-o matrice superior triangulară, adică de forma

$$\begin{pmatrix} a_{11} & a_{12} & \dots & \dots & a_{1m} \\ 0 & a_{22} & \dots & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & & & a_{mm} \end{pmatrix} \quad (5)$$

d. s. m. dacă toate valurile proprii ale lui T se află în K .

DEM. Dacă B este o bază a lui V în raport cu care $(T)_B$ este matricea $\Delta_T(\lambda) = (\lambda - \lambda_{11}) \cdots (\lambda - \lambda_{nn})$, deci T are n valori proprii în K .

Invers, presupunem că T are n valori proprii $\lambda_1, \dots, \lambda_n \in K$ (acestea sunt rădăcinile ecuației $\Delta_T(\lambda) = 0$, unde $A = (T)_B$, B o bază a lui V). Fie $v_1 \in V$ un vector propriu apartinând val. proprii λ_1 . Completăm mulțimea $\{v_1\}$ printr-o bază $B_1 = \{v_1, w_2^{(1)}, \dots, w_n^{(1)}\}$ a lui V . Matricea $A_1 = (T)_{B_1}$ este dată de relațiile

$$T(v) = \lambda_1 v_1$$

$$T(w_1^{(1)}) = a_{12}^{(1)} v_1 + a_{22}^{(1)} w_2^{(1)} + \dots + a_{nn}^{(1)} w_n^{(1)}$$

$$T(w_n^{(1)}) = a_{1n}^{(1)} v_1 + a_{2n}^{(1)} w_2^{(1)} + \dots + a_{nn}^{(1)} w_n^{(1)}$$

În expresiile lui $T(w_2^{(1)})$, ..., $T(w_n^{(1)})$ considerăm că sumele care sunt combinații liniare ale vectorilor $w_2^{(1)}, \dots, w_n^{(1)}$ definesc un operator liniar T_1 definit pe subspaceul $V_1 = L(w_2^{(1)}, \dots, w_n^{(1)})$ după cum urmează:

$$T_1(w_2^{(1)}) = a_{22}^{(1)} w_2^{(1)} + \dots + a_{nn}^{(1)} w_n^{(1)}$$

$$T_1(w_n^{(1)}) = a_{2n}^{(1)} w_2^{(1)} + \dots + a_{nn}^{(1)} w_n^{(1)}$$

Dovăzăce

$$A_1 = (T)_{B_1} = \begin{pmatrix} \lambda_1 & a_{12}^{(1)} & \dots & a_{1n}^{(1)} \\ 0 & a_{22}^{(1)} & \dots & a_{2n}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}^{(1)} & \dots & a_{nn}^{(1)} \end{pmatrix}$$

obs. că submatricea A_2 e liniară și, anume,

$$A_2 = \begin{pmatrix} a_{22}^{(1)} & \dots & a_{2n}^{(1)} \\ \vdots & & \vdots \\ a_{nn}^{(1)} & \dots & a_{nn}^{(1)} \end{pmatrix}$$

este matricea lui T_1 în baza $B_2 = \{w_2^{(1)}, \dots, w_n^{(1)}\}$ a lui V_1 . În plus, din

$$\Delta_T(\lambda) = \Delta_{A_1}(\lambda) \cdot (\lambda - \lambda_1) \Delta_{A_2}(\lambda) \quad \& \quad \Delta_{A_1}(\lambda) = \Delta_{T_1}(\lambda)$$

rezultă că $\Delta_T = (\lambda - \lambda_1) \dots (\lambda - \lambda_n)$, deci λ_2 este o valoare proprie a lui T_1 .

Fie $v_2 \in V_1$ un vector propriu al lui T_1 , deci $T_1(v_2) = \lambda_2 v_2$. Completăm $\{v_2\}$ până la o bază $B'_2 = \{v_2, w_3^{(2)}, \dots, w_n^{(2)}\}$ a lui V_1 . În raport cu această bază

$$A'_2 = (T)_{B'_2} = \begin{pmatrix} \lambda_2 & a'_{23} & \dots & a'_{2n} \\ 0 & a'_{33} & \dots & a'_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{nn} & \dots & a'_{nn} \end{pmatrix},$$

iar în baza lui V_1 , $B'_1 = \{v_1, v_2, w_3^{(2)}, \dots, w_n^{(2)}\}$ reprezentarea matricială a lui T este

$$(T)_{B'_1} = \begin{pmatrix} (1) & (2) & & (2) \\ \lambda_1 & a_{12} & a_{13} & \dots & a_{1n}^{(1)} \\ 0 & \lambda_2 & a_{23}^{(1)} & \dots & a_{2n}^{(1)} \\ 0 & 0 & a_{33}^{(2)} & \dots & a_{3n}^{(2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_{nn}^{(2)} & \dots & a_{nn}^{(2)} \end{pmatrix},$$

dovăzăce

$$T(v_1) = \lambda_1 v_1,$$

$$\begin{aligned} T(v_2) &= T(\alpha_2 w_2^{(1)} + \dots + \alpha_m w_m^{(1)}) \\ &= \alpha_2 T(w_2^{(1)}) + \dots + \alpha_m T(w_m^{(1)}) \\ &= \alpha_2 (a_{12}^{(1)} v_1 + a_{22}^{(1)} w_2^{(1)} + \dots + a_{m2}^{(1)} w_m^{(1)}) \\ &\quad + \alpha_3 (a_{13}^{(1)} v_1 + a_{23}^{(1)} w_2^{(1)} + \dots + a_{m3}^{(1)} w_m^{(1)}) \\ &\quad \vdots \\ &+ \alpha_m (a_{1m}^{(1)} v_1 + a_{2m}^{(1)} w_2^{(1)} + \dots + a_{mm}^{(1)} w_m^{(1)}) \\ &= (\alpha_2 a_{12}^{(1)} + \dots + \alpha_m a_{1m}^{(1)}) v_1 + \alpha_2 T_1(w_2^{(1)}) + \dots + \alpha_m T_1(w_m^{(1)}) \\ &= \alpha_{12}^{(2)} v_1 + T_1(w_2^{(1)}) \\ &= \alpha_{12}^{(2)} v_1 + \lambda_2 v_2, \end{aligned}$$

unde am notat $\alpha_{12}^{(2)} := \alpha_2 a_{12}^{(1)} + \dots + \alpha_m a_{1m}^{(1)}$. Un răționament similar celui pt T_1 se face pentru op. T_2 definit pe subsp $V_2 = L(w_3^{(2)}, \dots, w_m^{(2)})$ de dimensiune $n-2$. Continând, la final, construim și baza $B = \{v_1, \dots, v_{n-1}, w_m\}$ în raport cu care

$$(T)_{B_{n-1}} = \begin{pmatrix} \lambda_1 & a_{12}^{(n-1)} & & & & a_{1m}^{(n-1)} \\ 0 & \lambda_2 & & & & \\ 0 & 0 & \ddots & & & \\ 0 & 0 & \dots & \lambda_{m-1} & & a_{m-1m}^{(n-1)} \\ 0 & 0 & \dots & 0 & a_{mm}^{(n-1)} \end{pmatrix}$$

$$\Delta_T = (\lambda - \lambda_1) \cdots (\lambda - \lambda_{n-1})(\lambda - \lambda_n), \text{ deci } a_{mn}^{(n-1)} = \lambda_n.$$

11. EXEMPLU. Să arătăm că op. $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $T(x, y, z) = (-3x+y-z, -7x+5y-z, -6x+6y-2z)$ are o reprezentare matricială superior triangulară și să găsim o astfel de reprezentare. Matricea $A = (T)_B$, unde B este baza standard a lui \mathbb{R}^3 și pe care, în continuare, o notăm B_{01} , este

$$A = \begin{pmatrix} -3 & 1 & -1 \\ -7 & 5 & -1 \\ -6 & 6 & -2 \end{pmatrix}$$

$\Delta_T(\lambda) = \Delta(\lambda) = (\lambda+2)(\lambda-4)$. Din analiza Exemplului 2 avem $\dim V(-2) < 2$ prin urmare, T nu e diagonalizabil, respectiv matricea A nu este diagonalizabilă. Totuși, T are o reprezentare matricială superior triangulară pe care o vom determina urmând dem. Teor. 10.

Alegem $\lambda_1 = -2$ și găsim $v_1 = (1, 1, 0)$ vector propriu al lui λ_1 (a se vedea Exemplul 2). Completând mult. $\{v_1\}$ printr-o bază B_1 a lui \mathbb{R}^3 ,

de exemplu,

$$B_1 = \{v_1 = (1, 1, 0), w_2^{(1)} = (0, 1, 0), w_3^{(1)} = (0, 0, 1)\}.$$

Matr. $A_1 = (T)_{B_1}$ este dată de relație

$$T(v_1) = -2v_1,$$

$$T(w_2^{(1)}) = T(0, 1, 0) = (1, 5, 6) = (1, 1, 0) + (0, 4, 0) + (0, 0, 6) = 1 \cdot v_1 + 4 w_2^{(1)} + 6 w_3^{(1)},$$

$$T(w_3^{(1)}) = T(0, 0, 1) = (-1, -1, -2) = (-1, -1, 0) + (0, 0, -2) = -1 \cdot v_1 + 0 w_2^{(1)} - 2 w_3^{(1)},$$

pentru următoare,

$$A_1 = \begin{pmatrix} -2 & 1 & 1 \\ 0 & 4 & 0 \\ 0 & 6 & -2 \end{pmatrix}$$

Fie $V_1 = L(w_2^{(1)}, w_3^{(1)})$ și $T_1: V_1 \rightarrow V_1$ op. liniar definit prin

$$T_1(w_2^{(1)}) = 4 w_2^{(1)} + 6 w_3^{(1)}, \quad T_1(w_3^{(1)}) = 0 \cdot w_2^{(1)} + 2 w_3^{(1)}.$$

Scalărul $\lambda_2 = -2$ este o val. proprie a lui T_1 . Se determină $v_2 \in V_1$: fie

$$B_2 = \{w_2^{(1)}, w_3^{(1)}\} \text{ bază a lui } V_1. \text{ Dacă } T_1(v_2) = -2v_2 \text{ obținem } (T_1)_{B_2}(v_2) = -2(v_2)_{B_2}.$$

Punem $(v_2)_{B_2} = (x, y)$ și obținem

$$\begin{pmatrix} 4 & 0 \\ 6 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -2 \begin{pmatrix} x \\ y \end{pmatrix},$$

$$\begin{array}{l} 4x = -2x \\ 6x - 2y = -2y \end{array} \Leftrightarrow \left\{ \begin{array}{l} x = 0 \\ 6x = 0 \end{array} \right.$$

Alegem $(x, y) = (0, 1)$, de unde $v_2 = 0 \cdot w_2^{(1)} + w_3^{(1)} = (0, 0, 1)$. Completăm $\{v_2\}$ printr-o bază a lui V_1 , alegând $B' = \{v_2 = (0, 0, 1), w_3^{(2)} = (0, 1, 0)\}$. Acum

$B'' = \{v_1, v_2, w_3^{(2)} = (0, 1, 0)\}$ este o bază a lui \mathbb{R}^3 în raport cu care matricea superior triunghiulară $(T)_{B''}$ se determină din relație:

$$T(v_1) = -2v_1 = -2v_1 + 0 \cdot v_2 + 0 \cdot w_3^{(2)},$$

$$T(v_2) = T(0, 0, 1) = (-1, -1, -2) = (-1, -1, 0) + (0, 0, -2) = -1v_1 - 2v_2 + 0w_3^{(2)},$$

$$T(w_3^{(2)}) = T(0, 1, 0) = (1, 5, 6) = (1, 1, 0) + 6(0, 0, 1) + 4(0, 1, 0) = 1 \cdot v_1 + 6v_2 + 4w_3^{(2)}$$

Dacă,

$$(T)_{B''} = \begin{pmatrix} -2 & -1 & 1 \\ 0 & -2 & 6 \\ 0 & 0 & 4 \end{pmatrix}$$

Vectorul propriei v_3 corespunzătoare val. propriei $\lambda_3 = 4$ se obține din ec.

$$(T)_{B''}(v)_{B''} = 4(v)_{B''}$$

$$\begin{pmatrix} -2 & -1 & 1 \\ 0 & -2 & 6 \\ 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 4 \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \text{ unde am notat } (v)_{B''} = (x, y, z)$$

Rezultă sistemul

$$\begin{cases} -6x - y + z = 0 \\ -6y + 6z = 0 \end{cases} \Leftrightarrow \begin{cases} 6x + y - z = 0 \\ y - z = 0 \end{cases}$$

Obținem $v_3 = (0, 1, 1)$.

Subliniem că vectorii proprii ai lui T_1 , cum sunt orci v_2 și $w_3^{(1)}$, nu sunt vectori proprii ai lui T .

Matricea de trecere de la baza standard a lui \mathbb{R}^3 la baza B'' este data de relație,

$$v_1 = (1, 1, 0) = 1 \cdot e_1 + 1 \cdot e_2 + 0 \cdot e_3$$

$$v_2 = (0, 0, 1) = 0 \cdot e_1 + 0 \cdot e_2 + 1 \cdot e_3$$

$$w_3^{(1)} = (0, 1, 0) = 0 \cdot e_1 + 1 \cdot e_2 + 0 \cdot e_3$$

două

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

Astunci $P^{-1}AP = (T)_{B''}$, echivalent în relație $AP = P(T)_{B''}$.

(12) EXERCITIU. Fie $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $T(x, y, z) = (3x - 3y + 4z, -2x + 5y - 5z, -6x + 3y - 7z)$

- (a) Arătați că T are o reprezentare matricială superior triangulară;
 (b) Găsiți o reprezentare matricială superior triangulară.

(13) EXERCITIU. (A.P., p. 185). Fie $T: \mathbb{R}^4 \rightarrow \mathbb{R}^4$, $T(x_1, x_2, x_3, x_4) = (x_1 + x_4, x_2, x_3 - 2x_4, x_1 - 2x_3 + 5x_4)$

Aflați val. proprii $\lambda \in \mathbb{R}$, spațiiile proprii și anotăți că T e diagonalizabil.

Scrieți matr. P de trecere de la baza standard B la baza B' alcătuită din vectori proprii linian independenti.

Un vector $v \in \mathbb{R}^4$ are $(v)_B = (x_1, x_2, x_3, x_4)$. Dacă $(v)_{B'} = (y_1, y_2, y_3, y_4)$ este corespondator, avem deosebitiv că $T(x_1, x_2, x_3, x_4) = T(y_1, y_2, y_3, y_4)$.

Pentru $v = (1, 2, 3, 4)$ avem că $T(x_1, x_2, x_3, x_4) = T(y_1, y_2, y_3, y_4)$.

(14) EXERCITIU. Arătați că $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $T(x, y) = (x+y, y)$ nu e diagonalizabil, dar $T: \mathbb{C}^2 \rightarrow \mathbb{C}^2$, $T(z_1, z_2) = (z_1 + z_2, z_2)$ este diagonalizabil.

Reprezentări matriciale pentru sume directe de subsp. invariante

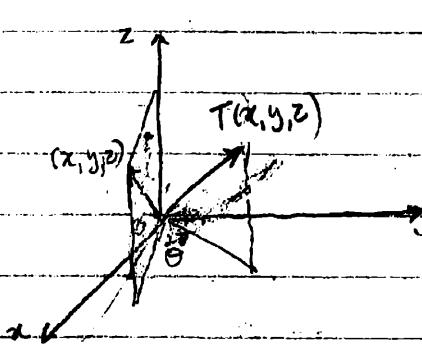
1. Subspatii invariante

Fie $T: V \rightarrow V$ un op. liniar. Subspatiul $W \subseteq V$ se numeste invariant față de T sau mai simplu, T -invariant dacă $T(W) \subseteq W$, adică $T(w) \in W$ pentru toti $w \in W$. În acest caz, restricția $T|_W : W \rightarrow V$ induce un operator $T_W : W \rightarrow W$ definit prin $T_W(w) := T(w)$, oricare ar fi $w \in W$.

(1) EXEMPLU. Transformarea liniară $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ date prin

$$T(x, y, z) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta, z)$$

roteste fiecare vector $v = (x, y, z) \in \mathbb{R}^3$ cu unghiul θ în jurul axei Oz (Fig. 1).



Planul $xOy = \{(x, y, 0) | x, y \in \mathbb{R}\}$ și, în general, planele $z = z_0$, parallele cu xOy sunt subspatii T -invariante. Un alt subspatiu T -invariant este axa $Oz = \{(0, 0, z) | z \in \mathbb{R}\}$. Transformarea $\tilde{T}: Oz \rightarrow Oz$ este aplicatia identitate.

(2) EXEMPLU. Fie $0 \neq v \in V$ un vector propriu al op. liniar $T: V \rightarrow V$ și presupunem că $T(v) = \lambda v$, $\lambda \in K$. Subspatiul propriu $V_\lambda = \{u \in V | T(u) = \lambda u\}$ este T -invariant. Mai mult, orice subspatiu T -invariant de dimensiune 1 este generat de un vector propriu. Într-o lecție, fie $W \subseteq V$ un subspatiu T -invariant, $W = \langle v \rangle = \tilde{L}(v) = \{\alpha v | \alpha \in K\}$. W fiind T -invariant, $T(v) \in W$ și fie $T(v) = \lambda v$. E clar că v este un vector propriu al val. proprii $\lambda \in K$.

Pentru ca să devenească furnizator de informații, este important să se enunță următoarele rezultate:

(3) TEOR. Fie $T: V \rightarrow V$ un op. liniar și $f(t)$ un polinom cu coef. în K .

Atunci nucleul $\text{Ker } f(T)$ al aplicatiei $f(T)$ este un subspatiu T -invariant.

Dem. Fie $f(t) = a_m t^m + \dots + a_1 t + a_0 \in K[t]$. Deci $v \in \text{Ker } f(T)$, atunci $a_m T^m(v) + \dots + a_1 T(v) + a_0 \text{Id}_V(v) = 0$. Aplicăm T egalității precedente

Dacă obținem că $T^m(T(v)) + \dots + a_1 T(v) + a_0 v = 0$, deci $T(v) \in \text{Ker } f(T)$. ■

Propoz. următoare este un prim pas în evidențierea unei proprietăți importante ale reprezentanțelor matricale ale subspațiilor T -invariante.

(4) PROP. Fie $T: V \rightarrow V$ op. liniar și $W \subseteq V$ un subsuplu T -invariant.

Dacă A este o reprezentare matricală a restricției $T_W: W \rightarrow W$, atunci T admite o reprezentare matricală cu blocuri de forma

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \quad (1)$$

Dem. Fie $\{w_1, \dots, w_r\} \subseteq W$ o bază a lui W . Extindem ac. bază la o bază $\{w_1, \dots, w_r, v_1, \dots, v_s\}$ a lui V . Matr. lui T în ac. bază se obține din relațiile:

$$T(w_1) = a_{11}w_1 + \dots + a_{1r}w_r$$

$$T(w_r) = a_{rr}w_r + \dots + a_{rr}w_r$$

$$T(v_1) = b_{11}w_1 + \dots + b_{1r}w_r + c_{11}v_1 + \dots + c_{1s}v_s$$

$$T(v_s) = b_{s1}w_1 + \dots + b_{sr}w_r + c_{s1}v_1 + \dots + c_{ss}v_s$$

Cu notăriile $A = (a_{ij})$, $B = (b_{ij})$ și $C = (c_{ij})$ matricea lui T în bazele $\{w_1, \dots, w_r, v_1, \dots, v_s\}$ este matricea (1).

2. Sumă directă

Un sp. vet. V este suma directă a subspațiilor sale W_1, \dots, W_r .

Dacă se scrie

$$V = W_1 \oplus W_2 \oplus \dots \oplus W_r,$$

dacă fiecare vector $v \in V$ poate fi scris ca o sumă

$$v = w_1 + w_2 + \dots + w_r, \quad (2)$$

că $w_i \in W_i$ ($1 \leq i \leq r$) unic determinată (se mai spune că scrisa (2) este unică).

(5) TEOR. Fie W_1, \dots, W_r subspații ale sv. V și presupunem că $\{w_{11}, \dots, w_{1m_1}\} \supseteq \dots \supseteq \{w_{rm_r}, \dots, w_{rm_r}\}$ sunt baze, respective, ale lui W_1, \dots, W_r . Atunci,

$V = W_1 \oplus \dots \oplus W_r \Leftrightarrow$ multimea $\{w_{11}, \dots, w_{1m_1}, \dots, w_{r1}, \dots, w_{rm_r}\}$ este o bază
a lui V cu $m_1 + \dots + m_r$ elemente.

Dem. Pres. că B este o bază a lui V . At. orice $v \in V$ se scrie, în mod unic

$$\vartheta = a_{11}w_{11} + \dots + a_{1m_1}w_{1m_1} + \dots + a_{r1}w_{r1} + \dots + a_{rm_r}w_{rm_r} = w_1 + \dots + w_r,$$

unde am notat $w_i = a_{i1}w_{i1} + \dots + a_{im_i}w_{im_i} \in W_i$, $i = \overline{1, r}$. Scrierea $v = w_1 + \dots + w_r$ este unică cu $w_i \in W$ deoarece coef. a_{ij} , $1 \leq j \leq m_i$, sunt unic determinate de v în serie.

$$\text{rez. } \vartheta = \sum_{i=1}^r \left(\sum_{j=1}^{m_i} a_{ij} w_{ij} \right).$$

Invers, presupunem că $V = W_1 \oplus \dots \oplus W_r$. At. orice $v \in V$ se scrie ca o sumă

$$\vartheta = w_1 + \dots + w_r, \text{ cu } w_i \in W_i \text{ unic determinat.}$$

In plus, fiecare w_i se scrie

$$w_i = a_{i1}w_{i1} + \dots + a_{im_i}w_{im_i}.$$

Pentru oricare, $v = \sum_{i,j} a_{ij} w_{ij}$ cu $w_{ij} \in B$, de unde

$v \in L(B)$. Se arată că mulțimea B este liniar independentă. Pt. acesta, fie

$$a_{11}w_{11} + \dots + a_{1m_1}w_{1m_1} + \dots + a_{r1}w_{r1} + \dots + a_{rm_r}w_{rm_r} = 0.$$

Dar $v \in V$ se scrie în mod unic $v = v_1 + \dots + v_r$ (deoarece, $v_i \in W_i$), urmășind că

$$a_{11}w_{11} + \dots + a_{1m_1}w_{1m_1} = 0, \quad i = \overline{1, r}.$$

rezultă că $a_{ij} = 0$, $j = \overline{1, m_i}$. In definitiv, toti $a_{ij} = 0$. ■

→

(A) TEOR. $V = W_1 \oplus \dots \oplus W_r \Leftrightarrow$

$$(a) V = W_1 + \dots + W_r$$

$$(b) W_i \cap (W_1 + \dots + W_{i-1} + W_{i+1} + \dots + W_r) = 0, \quad i = \overline{1, r}.$$

Dem. Exercițiu. ■

(8) DEF. Fie $T: V \rightarrow V$ opereator liniar. Dacă $V = W_1 \oplus \dots \oplus W_r$ este o sumă directă de

subspații T -invariante, adică $T(W_i) \subseteq W_i$, atunci spuneam că T este

suma directă a operatorilor $T_{W_i}: W_i \rightarrow W_i$ și se scrie $T = T_{W_1} \oplus \dots \oplus T_{W_r}$.

In aceste condiții se spune că T este decomponabil și că $T = T_{W_1} \oplus \dots \oplus T_{W_r}$ este o descompunere a lui T într-o sumă directă.

alese

(6) OBS. Descompunerea $V = W_1 \oplus \dots \oplus W_r$ este unică raportând-o la subspațiile

$W_1, \dots, W_r \subseteq V$. Altfel, V poate avea mai multe descomp. în sumă directă.

De exemplu, $\mathbb{R}^4 = \{(a, b, c, d) | a, b \in \mathbb{R}\} \oplus \{(0, 0, c, d) | c, d \in \mathbb{R}\}$ și, de asemenea, $\mathbb{R}^4 = \{(a, 0, c, 0) | a, c \in \mathbb{R}\} \oplus \{(0, b, 0, 0) | b \in \mathbb{R}\} \oplus \{(0, 0, d, 0) | d \in \mathbb{R}\}$.

Descompunerea op. $T: V \rightarrow V$ într-o sumă directă are drept consecință
o reprezentare matricială, dacă nu diagonală, atunci diagonală în blocuri,

în sensul propoz. următoare.

(9) PROP. Fie $T = T_1 \oplus \dots \oplus T_r$ o descompunere în sumă directă a operatorului liniar $T: V \rightarrow V$, corespunzătoare descompunerii în sumă directă de subspații T -invariante $V = W_1 \oplus \dots \oplus W_r$ cu $T_i = T|_{W_i}: W_i \rightarrow W_i$. Dacă A_i este o reprezentare matricială a lui T_i , atunci T are o reprezentare matricială de formă

$$A = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & A_r \end{pmatrix} \quad (1)$$

adică o reprezentare matricială diagonală cu blocuri $A_i \in M_{m_i}(K)$, unde $m_i = \dim_K W_i$, $1 \leq i \leq r$.

Dem. Pentru simplitate presupunem că $T = T_1 \oplus T_2$, $\dim W_1 = 2$ cu $B_1 = \{w_{11}, w_{12}\}$ bază a lui W_1 și $\dim W_2 = 3$ cu $B_2 = \{w_{21}, w_{22}, w_{23}\}$ bază a lui W_2 .

Dacă $T_1(w_{11}) = a_{11}w_{11} + a_{21}w_{12}$ și $T_1(w_{12}) = a_{12}w_{11} + a_{22}w_{12}$, atunci

$$A_1 = (T_1)_{B_1} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Analog, se obține

$$A_2 = (T_2)_{B_2} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$$

Cu Teor. 5 avem că $B = B_1 \cup B_2$ este o bază a lui B . Înțeles că dacă $T(w_{ij}) = T_1(w_{ij})$ rezultă că

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

Polinomul minimal

al unui op. T

Polinomul caracteristic și polinomul minimal furnizează reprezentanțe matriciale (1) în blocuri-matrice sau celule-matrice de o formă suficient de bună pentru ca matricea A să fie căt mai apropiată de o matrice diagonală. Pentru simplitate, mai întâi vom concentra studiul asupra polinomului minimal al unei matrice patrate.

Fie $A \in M_n(K)$. Din Teor. Hamilton-Cayley rezultă că există polinoame nenule $f \in K[\lambda]$ care au A ca radici, adică $f(A) = 0$, unde f este polinomul caracteristic $\Delta_A(\lambda)$.

(10) PROP. Există un polinom monic de gradul cel mai mic, unic determinat care are matricea $A \in M_n(K)$ ca rădine în multimea $M_n(K)$. Acest polinom îl numim polinomul minimal al lui A și îl notăm $m_A(\lambda)$.

Dem. Fie $P = \{m \in \mathbb{N} \mid \text{există un polinom de gradul } m \text{ care are } A \text{ ca rădine}\}$.
 $P \neq \emptyset$ deoarece $\text{grad}(\Delta_A(\lambda)) \in P$. Este o submultime a multimii bine ordonate $\mathbb{N} \Rightarrow \exists \min P = n_0 \in P$. Fie $f \in K[\lambda]$ a.s. $\text{grad}(f) = n_0$ și $f(A) = 0$. Impărțim f la coefficientul său dominant și obținem un polinom monic $m_A(\lambda)$ cu $m_A(A) = 0$. Polinomul $m_A(\lambda)$ este unic deoarece dacă $m'(\lambda)$ este un alt polinom monic de grad n_0 cu $m'(A) = 0$, atunci $m_A(\lambda) - m'(\lambda)$ este un polinom de grad $< n_0$ care se anulează în A , contradicție cu minimitatea lui n_0 . ■

(11) PROP. Polinomul minimal $m_A(\lambda)$ al matricei $A \in M_n(K)$ divide orice polinom care are pe A rădine. În particular, $m_A(\lambda) \mid \Delta_A(\lambda)$.

Dem. Fie $f(\lambda) \in K[\lambda]$ a.s. $f(A) = 0$. Din teor. împărțirea cu rest, $f(\lambda) = m_A(\lambda) \cdot q(\lambda) + r(\lambda)$, unde $q, r \in K[\lambda]$, iar $r = 0$ ori $r \neq 0$ și $\text{grad}(r) < \text{grad}(m_A(\lambda))$. Dacă $r \neq 0$, atunci $f(A) = m_A(A) \cdot q(A) + r(A) \Rightarrow r(A) = 0$, contradicție cu minimitatea gradului lui $m_A(\lambda)$. ■

(12) LEMĂ. $\Delta_A(\lambda) \mid (m_A(\lambda))^n$, $\forall A \in M_n(K)$.

Dem. Fie $m_A(\lambda) = \lambda^r + c_1\lambda^{r-1} + \dots + c_r$. Căutăm o matrice $B(\lambda) = \lambda^k B_0 + \lambda^{k-1} B_1 + \dots + \lambda B_{k-1} + B_k$ a.s. $(\lambda I - A)B(\lambda) = M_A(\lambda) \cdot I$. Din identificarea coeficienților lui λ obținem că $k = r-1$, $B_0 = I$, $B_1 = A + c_1 I$, $B_2 = A^2 + c_1 A + c_2 I$, \dots , $B_{r-1} = A^{r-1} + c_1 A^{r-2} + \dots + c_{r-1} I$. Acum, din rel. $|\lambda I - A| \cdot |B(\lambda)| = (m_A(\lambda))^n$ rezultă $\Delta_A(\lambda) \mid (m_A(\lambda))^n$. ■

(13) PROP. Polinomul minimal $m_A(\lambda)$ are același factori ireductibili ca și polinomul caracteristic $\Delta_A(\lambda)$.

Dem. Fie $f(\lambda) \in K[\lambda]$ un polinom ireductibil peste K . Dacă $f(\lambda) \mid m_A(\lambda)$, atunci

este clar că $f(\lambda) \mid \Delta_A(\lambda)$. Învers, să presupunem că $f(\lambda) \mid \Delta_A(\lambda)$. Atunci, din Lemă 12 rezultă că $f(\lambda) \mid (m_A(\lambda))^n$. Cum $f(\lambda)$ este ireductibil deducem că $f(\lambda) \mid m_A(\lambda)$. ■

(14) COR. (a) $\lambda \in K$ este val. proprie a matricei $A \Leftrightarrow \lambda$ este rădăcină a polinomului minimal $m_A(\lambda)$.

(b) Mai general, dacă $\Delta_A(\lambda) = (f_1(\lambda))^{m_1} \cdots (f_r(\lambda))^{m_r}$, unde $f_i(\lambda)$ sunt polinoame ireductibile, atunci $m_A(\lambda) = (f_1(\lambda))^{m_1} \cdots (f_r(\lambda))^{m_r}$, cu $m_i \leq M_i$, $i=1, \dots, r$.

(15) EXEMPLU. Să găsim polinomul $m_A(\lambda)$ pentru $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$.

Aveam $\Delta_A(\lambda) = (\lambda-2)^3(\lambda-5)$. Conform Prop. 13, $m_A(\lambda)$ poate fi unul din polinoamele $m_1(\lambda) = (\lambda-2)(\lambda-5)$, $m_2(\lambda) = (\lambda-2)^2(\lambda-5)$, $m_3(\lambda) = (\lambda-2)^3(\lambda-5) = \Delta_A(\lambda)$. Este clar că $m_3(A) = 0$. Apoi, $m_1(A) = (A-2I)(A-5I)$ și efectuând calculile obținem

$$m_1(A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} -3 & 1 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -3 & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix} \neq 0.$$

Apoi,

$$m_2(A) = (A-2I)^2(A-5I) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} -3 & 1 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 0,$$

deci $m_2(\lambda) = (\lambda-2)^2(\lambda-5)$.

(16) OBS. Polinomul minimal al op. liniar $T: V \rightarrow V$, dim $V = n$, este polinomul minimal al oricărui reprezentător matricial a lui T . Într-adevăr, dacă A este o reprez. matricială a lui T și $m_A(\lambda) = \lambda^r + c_1\lambda^{r-1} + \cdots + c_r\lambda + c_r$, atunci $m_A(\lambda) = A^r + c_1A^{r-1} + \cdots + c_rA + c_rI = 0$. Acum, dacă $A = P^{-1}AP$ este o altă reprezentare matricială a lui T , atunci $m_A(A') = P^{-1}m_A(A)P = 0 \Rightarrow m_{A'}(\lambda) \mid m_A(\lambda)$. Analog, se arată că $m_{A'}(\lambda) \mid m_{A''}(\lambda)$, deci $m_{A''}(\lambda) = m_{A'}(\lambda)$.

Pă de altă parte, amintim că dacă $A = (T)_B$, atunci $A^r + c_1A^{r-1} + \cdots + c_rA + c_rI = 0 \Leftrightarrow (T)_B^r + c_1(T)_B^{r-1} + \cdots + c_r(T)_B + c_rI = 0 \Leftrightarrow ((T)_B^r + c_1(T)_B^{r-1} + \cdots + c_r(T)_B + c_rI)(v)_B = 0, \forall v \in V \Leftrightarrow T(v) + c_1T^{r-1}(v) + \cdots + c_rT(v) + c_rv = 0, \forall v \in T \Leftrightarrow T^r + c_1T^{r-1} + \cdots + c_rT + c_rId_V = 0$, adică T este nul a lui $m_{A''}(\lambda)$.

H.B. $(T \circ T \circ \cdots \circ T)_B = (T)_B \cdot (T)_B \cdots (T)_B$, adică matricea compunerii este egală cu produsul matricelor.

Descompunere primară

este ocaz

Rezultatul principal al acestui paragraf este că polin. minimalul al op. liniar $T: V \rightarrow V$, mai exact descompunerea sa în factori ireductibili, este supratul unei descompuneri a lui V într-o sumă directă de subspații T -invariante.

(17) LEMĂ. Fie $T: V \rightarrow V$ un op. liniar și fie $f(\lambda) \in K[\lambda]$ un polinom cu proprietăți $f(t) = 0$ și $f(\lambda) = g(\lambda)h(\lambda)$ este o descompunere într-un modus de polin. relativ prime. Atunci $V = \text{Ker } g(T) \oplus \text{Ker } h(T)$ este o sumă directă de subspații T -invariante.

Dem. Din Teo. 3 rezultă că $W_1 = \text{Ker } g(T)$ și $W_2 = \text{Ker } h(T)$ sunt T -invariante.

Așa cămăs $V = W_1 + W_2$: pt. acesta, fie $r(\lambda)$ și $s(\lambda) \in K[\lambda]$ s.t. $r(t)g(t) + s(t)h(t) = 1$.

Atunci $r(T)g(T) + s(T)h(T) = 1_V$, respectiv $r(T)g(T)(v) + s(T)h(T)(v) = 0$, $\forall v \in V$.

Vect. $r(T)g(T)(v) \in W_2$ deoarece $h(T)r(T)g(T) = r(T)(h(T)g(T)) = r(T)f(T) = 0$.

Analog, $s(T)h(T)(v) \in W_1$. În consecință, $V = W_1 + W_2$. Sumă $W_1 + W_2$ este directă dacă $v = w_1 + w_2$, cu w_i unic determinat. Așa cămăs $r(T)g(T)$ lui $v = w_1 + w_2$ obținem $r(T)g(T)(v) = r(T)g(T)(w_1) + r(T)g(T)(w_2) = r(T)g(T)(w_2)$. Pe de altă parte, din $r(T)g(T) + s(T)h(T) = 1_V$ rezultă $r(T)g(T)(w_2) + s(T)h(T)(w_2) = w_2$, deci $r(T)g(T)w_2 = w_2$. Astăndăt, $r(T)g(T)(v) = w_2$, deci w_2 este unic determinat de v .

Analog, se arată că $s(T)h(T)(v) = w_1$. În definitie, $v = w_1 + w_2$ cu $w_i \in W_i$, unic determinat de v . ■

(18) LEMĂ. În condițiile Lemei 17, dacă $f(\lambda)$ este polinomul minimal al lui T , iar $g(\lambda)$ și $h(\lambda)$ sunt monice, atunci $g(\lambda)$ este polinomul minimal al restricției $T_1 = T|_{W_1}$ și $h(\lambda)$ este polinomul minimal al restricției $T_2 = T|_{W_2}$, unde $W_1 = \text{Ker } g(T)$, $W_2 = \text{Ker } h(T)$.

Dem. Fie $m_i(\lambda)$ polin. minimal al lui T_i , $i=1,2$. Din relația $f(T_i)(w_i) = f(T)(w_i) = 0$, $\forall w_i \in W_i$ rezultă că T_i este un zero al polinomului f .

Atunci, $m_i(\lambda) | f(\lambda)$, $i=1,2$. În continuare, vom arăta că $f(\lambda) = m_1(\lambda) \cdot m_2(\lambda)$.

Pentru aceasta, fie $\alpha(\lambda)$ un multiplu comun al polinoamelor $m_1(\lambda)$ și $m_2(\lambda)$.

Atunci, $\alpha(T_1)(W_1) = 0$ și $\alpha(T_2)(W_2) = 0$. Fie $v = w_1 + w_2$, $w_i \in W_i$. Avem

$\alpha(T)(v) = \alpha(T)w_1 + \alpha(T)w_2 = \alpha(T_1)w_1 + \alpha(T_2)w_2 = 0 + 0 = 0$, pt. orice $v \in V$.

Ac. înseamnă că T este un zero al polin. $\alpha(\lambda)$, deci $f(\lambda) | \alpha(\lambda)$.

Așa arătat că $f(\lambda)$ este un multiplu comun al polinoamelor relativ prime

$m_1(\lambda) \mid m_2(\lambda)$ și orice alt multiplu comun al lor este multiplu al lui $f(\lambda)$. Rezultă că $f(\lambda) = c \cdot m \cdot m \cdot m.c. (m_1(\lambda), m_2(\lambda)) = m_1(\lambda) m_2(\lambda)$. În definitie, $g(\lambda) := m_1(\lambda)$ și $h(\lambda) = m_2(\lambda)$. ■ :

(19) TEOR (de descompunere primară). Fie $T: V \rightarrow V$ un operator liniar cu polin. minimal

$$m_p(\lambda) = (f_1(\lambda))^{m_1} (f_2(\lambda))^{m_2} \cdots (f_r(\lambda))^{m_r},$$

unde $f_i(\lambda)$ sunt polinoame ireductibile distințe. At. V este suma directă a subspațiilor T -invariante W_1, \dots, W_r , unde $W_i = \text{Ker } f_i(T)^{m_i}$.

Mai mult, $(f_i(t))^{m_i}$ este polinomul minimal al restricției $T_i := T|_{W_i}$.

Dem. Inductie după r . Casul $r=1$ este clor. Pres. teor. adică pt $r=1$ și dem.

pentru r . Aplicăm lema 17 polinomului $m(\lambda) = (f(\lambda))^{m_1} \cdot f(\lambda)$, unde $f(\lambda) = (f_2(\lambda))^{m_2} \cdots (f_r(\lambda))^{m_r} : V = W_1 \oplus V_1$, unde $W_1 = \text{Ker } f_1(T)^{m_1}$ și $V_1 = \text{Ker } f(T)$. Cf. lemei 17, $(f_1(\lambda))^{m_1}$ este polin. minimal al restricției $T|_{W_1}$, iar $f(t)$ este polin. minimal al restricției $T_1 = T|_{V_1}$.

Cu ipoteza de inducție V_1 este suma directă $V_1 = W_2 \oplus \cdots \oplus W_r$, unde

$W_i = \text{Ker } f_i(T_1)^{m_i}$ și $f_i(\lambda)$ este polin. minimal al lui $T_i = T_1|_{W_i}$, $i = 2, \dots, r$. Deoarece $(f_i(\lambda))^{m_i} \mid f(\lambda) \Rightarrow \text{Ker } f_i(T)^{m_i} \subseteq \text{Ker } f(T) = V_1$, $i = 2, \dots, r$. Pentru că pe V_1 operatorii

T_1 și T lucresc la fel pe V_1 obținem că $\text{Ker } f_i(T)^{m_i} = \text{Ker } f_i(T_1) = W_i$ și că

$f_i(T)^{m_i}$ este polinomul minimal al lui $T|_{W_i}$, $i = 2, \dots, r$. În definitie,

descompunerea $V = W_1 \oplus \cdots \oplus W_r$ îndeplinește condiția din enunțul teoremei. ■

Forma canonica Jordan

Teorema de descompunere primară (Teor 18 din L5) este vîrful principalei construcții pe cele 17 enunțuri care se precead în lecția precedentă. Pominând de la descompunerea polinomului minimul $m_T(\lambda)$ al op. liniară $T: V \rightarrow V$, avem

$$m_T(\lambda) = (f_1(\lambda))^{n_1} \cdots (f_r(\lambda))^{n_r},$$

unde $f_i(\lambda)$ sunt polinoame ireductibile distințe, obținute următoarele:

- (a) $V = W_1 \oplus \cdots \oplus W_r$, unde $W_i = \text{Ker}(f_i(T))^{n_i}$ este T -invariant;
- (b) polinomul $(f_i(\lambda))^{n_i}$ este polinomul minimul al restricției $T_i = T|_{W_i}$.

Mei mult, dacă B_i este o bază a lui W_1, \dots, B_r este o bază a lui W_r , atunci $B = B_1 \cup \dots \cup B_r$ este o bază a lui V (cf. Teor 5). În fine, Prop. 9 ne arătă că T are o reprezentare matricială diagonală cu blocuri, mai exact,

$$\begin{matrix} (T) \\ B \end{matrix} = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & A_r \end{pmatrix}.$$

Din teor. de descomp. primară, polinomul $(f_i(\lambda))^{n_i}$ este polinomul minimul $m_{T_i}(\lambda)$ al restricției T_i , deci $(f_i(T_i))^{n_i} = 0$ (fecară preuzem că $f_i(\lambda) \neq 0$, deci T este definit pe V , pe cănd T_i este definit pe subspacele $W_i \subset V$). Relația $(f_i(T_i))^{n_i} = 0$ înseamnă că op. liniar $f_i(T_i)$ este nilpotent. În continuare, ne vom concentra asupra op. liniar nilpotenți, cu scopul de a completa descomp. primară a lui V cu proprietăți specifice ale op. nilpotenți $f_i(T_i): W_i \rightarrow W_i$, $1 \leq i \leq r$.

Operatori nilpotenți

Op. liniar $T: V \rightarrow V$ s.m. nilpotent dacă există un întreg $m \geq 1$ s.t. $T^m = 0$, adică $(T \circ T \circ \dots \circ T)(v) = 0$, pt. orice $v \in V$. Integru porția k pt care $T^k = 0$, dar $T^{k-1} \neq 0$ s.m. indicele de nilpotență al lui T .

(1) EXEMPLU. Fie $T: \mathbb{R}^4 \rightarrow \mathbb{R}^4$, $T(x_1, x_2, x_3, x_4) = (x_2 + x_3 - x_4, 2x_3 + 3x_4, 5x_4, 0)$.

Din compunerile $(x_1, x_2, x_3, x_4) \xrightarrow{T} (x_2+x_3-x_4, 2x_3+3x_4, 5x_4, 0) \xrightarrow{T}$
 $\xrightarrow{T} (2x_3+8x_4, 10x_4, 0, 0) \xrightarrow{T} (10x_4, 0, 0, 0) \xrightarrow{T} (0, 0, 0, 0)$ rezulta că
 $T^4 = 0$ și $T^3 \neq 0$. Deci, indicele de nilpotență a lui T este 4.

Dacă indicele de nilpotență a lui $T: V \rightarrow V$ este k , atunci oricare ar fi B o bază a lui V pe care $T(v) = 0$ rezultă relația

$$0 = (T^k(v))_B = (T^k)_B(v)_B = (T)_B^k(v)_B, \quad \forall v \in V.$$

Punând în rel. precedentă succesiiv vectorii corespondenți pt. fiecare vect. al lui B , adică $(v)_B = (1, 0, \dots, 0)$, $(v)_B = (0, 1, \dots, 0)$, ..., $(v)_B = (0, 0, \dots, 0, 1)$ se obține $(T)_B^k = 0$. De aceea, noi definim de nilpotență se definește, în mod natural, și pentru matricele patrate: matr. $A \in M_n(k)$ este nilpotent dacă $\exists m \geq 1$ s.t. $A^m = 0$. Cel mai mic întreg $m \geq 1$ pt. care $A^m = 0$ s.n. indicele de nilpotență al matricei A . Un exemplu de matrice nilpotentă este

$$A = \begin{pmatrix} 0 & 1 & -1 & 0 & 1 \\ 0 & 0 & 4 & 5 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

O particularitate a unui oper. nilpotent / matr. nilpotentă este că polinomul minimul este $m(\lambda) = \lambda^k$, k fiind indicele de nilpotență. Într-adevăr, dacă T ar avea o valoare proprie $\lambda_0 \neq 0$, iar $v_0 \neq 0$ ar fi un vector propriu al său, atunci din $T(v_0) = \lambda_0 v_0$ rezulta că $T^m(v_0) = \lambda_0^m v_0 \neq 0$ pentru orice $m \geq 1$, în contradicție cu constituția $T^k(v) = 0$, $\forall v \in V$. De aceea $m(\lambda) = \lambda^k$ rezultă că $\lambda = 0$ este unică val. proprie a unui oper. nilpotent / matr. nilpotentă.

- (e) PROP. Fie $v \in V$ s.t. $T^k(v) = 0$, dar $T^{k-1}(v) \neq 0$ (deci, vectorii $v, T(v), \dots, T^{k-1}(v)$ sunt nenuli și $T^k(v) = 0$). Atunci,
 - (i) Multimea $S = \{v, T(v), \dots, T^{k-1}(v)\}$ este liniar independentă.
 - (ii) Subspatiul $W = L(S)$ este T -invariant.
 - (iii) Restricția $\hat{T} := T|_W : W \rightarrow W$ este oper. nilpotent de indice k .
 - (iv) Reprezentarea matricială $(\hat{T})_S$ în raport cu baza ordonată $S = (T^{k-1}(v), \dots, T(v), v)$ este matricea patratică de ordinul k ,

$$\begin{pmatrix} \hat{T} \\ \vdots \end{pmatrix}_S = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

care are indicele de nilpotență egal cu k .

Dem. (i) Fie $\alpha_0 v + \alpha_1 T(v) + \dots + \alpha_{k-1} T^{k-1}(v) = 0$, unde $\alpha_i \in K$. Aplicăm T^{k-1} acestei egalități și obținem $\alpha_0 T^{k-1}(v) = 0$, prin urmare $\alpha_0 = 0$. Mai departe, aplicăm T^{k-2} egalității $\alpha_1 T(v) + \dots + \alpha_{k-1} T^{k-1}(v) = 0$ și obținem $\alpha_1 = 0$. Dacă k par, obținem $\alpha_0 = \alpha_1 = \dots = \alpha_{k-1} = 0$.

(ii) Fie $w \in W$, $w = \alpha_0 v + \alpha_1 T(v) + \dots + \alpha_{k-1} T^{k-1}(v)$. At. $T(w) = \alpha_0 T(v) + \alpha_1 T^2(v) + \dots + \alpha_{k-2} T^{k-1}(v) \in W$.

(iii) Dacă v satisface $T(v) = 0$, deci $w = \alpha_0 v + \alpha_1 T(v) + \dots + \alpha_{k-1} T^{k-1}(v)$, atunci $\hat{T}(w) = T(w)$ și $\hat{T}(w) = T(w) = \alpha_0 T(v) + \dots + \alpha_{k-1} T^{k-1}(v) = 0$; dacă $\hat{T}^{k-1} \neq 0$ și $\hat{T}^{k-1}(v) \neq 0$.

(iv) Matricea $(\hat{T})_S$ se obține aplicând succesiiv \hat{T} pe baza ordonată S . Astfel $\hat{T}(T^{k-1}(v)) = T^{k-1}(v) = 0 = 0 \cdot T^{k-1}(v) + 0 \cdot T^{k-2}(v) + \dots + 0 \cdot T(v) + 0 \cdot v$, $\hat{T}(T^{k-2}(v)) = T^{k-2}(v) = 1 \cdot T^{k-1}(v) + 0 \cdot T^{k-2}(v) + \dots + 0 \cdot T(v) + 0 \cdot v$, \dots , $\hat{T}(v) = T(v) = 0 \cdot T^{k-1}(v) + 0 \cdot T^{k-2}(v) + \dots + 1 \cdot T(v) + 0 \cdot v$.

Prin urmare,

$$\begin{pmatrix} \hat{T} \\ \vdots \end{pmatrix}_S = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix} \in M_{k \times k}(K).$$

Cititorul poate verifica relațiile $(\hat{T})_S^{k-1} = 0$ și $(\hat{T})_S^k = 0$.

LEMĂ 2. Fie $T: V \rightarrow V$ op. liniar. Putem $U := \text{Ker } T^t$, $W := \text{Ker } T^{t+1}$. Atunci, $U \subseteq W$ și $T(W) \subseteq U$.

Dem. Exercițiu.

LEMĂ 3. Fie $T: V \rightarrow V$ liniar. Putem $X = \text{Ker } T^{t-2}$, $Y = \text{Ker } T^t$, $Z = \text{Ker } T^{t+1}$. Atunci,

(i) $X \subseteq Y \subseteq Z$;

(ii) $Z = X \cup Y$.

$$\{u_1, \dots, u_r\}, \{u_1, \dots, u_r, v_1, \dots, v_s\}, \{u_1, \dots, u_r, v_1, \dots, v_s, w_1, \dots, w_t\}$$

sunt baze ale lui X , Y și Z , atunci multimea

$$S = \{u_1, \dots, u_r, T(v_1), \dots, T(v_s)\}$$

este conținută în Y și este liniar independentă.

Dem. Din lema 2, $T(Z) \subset Y$, prin urmare $S \subseteq Y$. Pres. că S este liniar dependentă. Atunci există o comb. liniară

$$\alpha_1 u_1 + \dots + \alpha_r u_r + b_1 T(w_1) + \dots + b_t T(w_t) = 0$$

cu cel puțin un coef. nenul. Mai mult, cel puțin un coef. $b_k \neq 0$ devine că $\{u_1, \dots, u_r\}$ este lin. indep. Mai departe, avem

$$b_1 T(w_1) + \dots + b_t T(w_t) = -\alpha_1 u_1 - \dots - \alpha_r u_r \in \text{Ker } T^{i-2}$$

$$\text{de unde } T^{i-2}(b_1 T(w_1) + \dots + b_t T(w_t)) = 0.$$

Rezultă că $T^{i-1}(b_1 w_1 + \dots + b_t w_t) = 0$, respectiv $w = b_1 w_1 + \dots + b_t w_t \in \text{Ker } T^{i-1} = Y$.

Ca element al lui Y , w se scrie ca o comb. liniară a vectorilor u_i, v_j , adică

$$w = \alpha_1 u_1 + \dots + \alpha_r u_r + \beta_1 v_1 + \dots + \beta_s v_s.$$

Rezultă că

$$\alpha_1 u_1 + \dots + \alpha_r u_r + \beta_1 v_1 + \dots + \beta_s v_s + (-b_1) w_1 + \dots + (-b_t) w_t = 0,$$

cu cel puțin un $b_k \neq 0$. Contradicție. ■

TEOR. 4. Fie $T: V \rightarrow V$ liniar de indice de nilpotență r . Atunci T are o reprezentare matricială diagonală cu blocuri de forma

$$H = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}. \quad (1)$$

Cel puțin un bloc H are ordinul r , iar celelalte blocuri au ordinul $\leq r$. Nr.

blocurilor H de fiecare ordin posibil este unic determinat de T , iar nr. tuturor blocurilor este egal cu defectul lui T , adică cu $\dim_K(\text{Ker } T)$. În fapt, nr. blocurilor H de ordin i este $2m_i - m_{i+1} - m_{i-1}$, unde $m_i = \dim_K(\text{Ker } T^i)$, pt. $1 \leq i \leq r$, al blocurilor de ordin r este $m_r - m_{r-1}$, al blocurilor de ordin 1 este $2m_1 - m_2$.

Dem. Fie $\dim_K V = n$. Punem $W_1 = \text{Ker } T$, ..., $W_r = \text{Ker } T^r$ și notăm $m_i = \dim_K W_i$, $i=1, \dots, r$.

Pentru că indice de nilpotență al lui T este r se obține că $W_r = V$, iar $W_{r-1} \neq V$. Prin urmare, $m_{r-1} < m_r = n$. Din Lema 3 avem următorul strict ascendent

$$W_1 \subset W_2 \subset \dots \subset W_r = V. \quad (2)$$

Vom căuta o bază a lui V în raport cu care T are reprezentarea matricială dorită pornind de la o bază $B = \{u_1, \dots, u_m\}$ a lui V și $\{v_1, \dots, v_{m-r}\}$ este o bază a lui W_i , $i=1, \dots, r$. Scriem vectorii bazei B sub forma

$$B = \{u_1, \dots, u_{m-r-2}, v_1, \dots, v_{m-r-1-m_{r-2}}, w_1^r, \dots, w_{m_r-m_{r-1}}^r\}$$

unde am notat

$$v_i = u_{m-r-2+i} \quad și \quad w_j^r = u_{m-r-1+j}.$$

Cu Lema 3 rezultă că multimea

$$S_1 = \{u_1, \dots, u_{m_{r-2}}, T(w_1^{(r)}), \dots, T(w_{m_r - m_{r-1}}^{(r)})\} \subset W_{r-1}.$$

este liniară îndep. Completăm S_1 până la o bază a lui W_{r-1} , pe care să scriem, după o renumențare a vectorilor $T(w_1^{(r)}), \dots, T(w_{m_r - m_{r-1}}^{(r)})$ și a celor ce completează baza lui W_{r-1} , sub forma

$$B_1 = \{u_1, \dots, u_{m_{r-3}}, v_1, \dots, v_{m_{r-2} - m_{r-3}}, w_1^{(r-1)}, \dots, w_{m_{r-1} - m_{r-2}}^{(r-1)}\}$$

unde $v_i = u_{m_{r-2}+i}$, $i=1, \dots, m_r - m_{r-1}$, împreună cu căi care completează baza lui W_{r-1} .

Apliind din nou Lema 3 și obținem că

$$S_2 = \{u_1, \dots, u_{m_{r-3}}, T(w_1^{(r-1)}), \dots, T(w_{m_{r-1} - m_{r-2}}^{(r-1)})\} \subset W_{r-2}$$

este o mulțime liniară îndep. Completăm S_2 până la o bază a lui W_{r-2} , pe care, după o renumențare a vectorilor $T(w_1^{(r-1)}), \dots, T(w_{m_{r-1} - m_{r-2}}^{(r-1)})$ și a căi ce completează baza lui W_{r-2} , să scriem sub forma

$$B_2 = \{u_1, \dots, u_{m_{r-4}}, v_1, \dots, v_{m_{r-3} - m_{r-4}}, w_1^{(r-2)}, \dots, w_{m_{r-2} - m_{r-3}}^{(r-2)}\},$$

unde $v_i = u_{m_{r-4}+i}$, $i=1, m_{r-3} - m_{r-4}$, $w_j^{(r-2)} = T(w_{j-1}^{(r-1)})$, $j=1, m_{r-1} - m_{r-2}$. Continuând în acest mod obținem veit.

$$w_1^{(r-1)}, \dots, w_{m_r - m_{r-1}}^{(r-1)}$$

$$w_1^{(r-1)}, \dots, w_{m_r - m_{r-1}}^{(r-1)}, \dots, w_{m_{r-1} - m_{r-2}}^{(r-1)}, \dots, w_{m_2 - m_1}^{(r-1)}, \dots, w_{m_r}^{(r-1)}$$

(3)

$$w_1^{(r-1)}, \dots, w_{m_r - m_{r-1}}^{(r-1)}, \dots, w_{m_{r-1} - m_{r-2}}^{(r-1)}, \dots, w_{m_2 - m_1}^{(r-1)}, \dots, w_{m_r}^{(r-1)}$$

care sunt liniară îndep. datorită inclusiunii stricte (2). Vectorii ultimii

linii alcătuiesc o bază pt W_1 , apoi cei din ultima și penultima linie

alcătuiesc o bază pt W_2 etc. Să observăm că fiecare dintre vectorii unei coloane, exceptându-l pe cel mai de sus, este imaginea călăzită de

deasupra sa; de exemplu, $w_1^{(r-1)} = T(w_1^{(r)})$, $w_2^{(r-2)} = T(w_1^{(r-1)})$, ..., $w_1^1 = T(w_1^{(2)})$,

astfel că prima coloană este alcătuită din vectorii

$$w_1^{(r)}, T(w_1^{(r)}), T^2(w_1^{(r)}), \dots, T^{r-1}(w_1^{(r)})$$

Cu această precizare, scriind baza lui V ca mulțime ordonată

$$(w_1^{(r)}, \dots, w_1^{(r)}, w_2^{(r)}, \dots, w_2^{(r)}, \dots, \dots)$$

obținem o matrice diagonală cu blocuri de forme (1), cf. Prop. 1(iv).

Din linile teoremei (3) determinăm numărul blocurilor de un anumit ordin. Astfel, din linia întâi deducem că sunt $m_r - m_{r-1}$ blocuri H de

ordinalul r_2 din limitele $1 \leq i \leq 2$ deducem că sunt $(m_{r_1} - m_{r_2}) - (m_r - m_{r-1}) = 2m_{r-1} - m_r - m_{r-2}$ blocuri de ordin $r-1$, ..., $2m_2 - m_3 - m_1$ blocuri de ordinul 2 și $2m_1 - m_2$ blocuri de ordinul 1.

In fine, numărul blocurilor este suma

$$(m_r - m_{r_1}) + [(m_{r-1} - m_{r_2}) + (m_r - m_{r-1})] + \dots + [(m_2 - m_1) - (m_3 - m_2)] + [m_1 - (m_2 - m_1)] \\ = m_1, \text{ deci } \dim(\ker T), \text{ devine } W_1 = \ker T.$$

APLICATIUA 5. Vom determina forma canonică diagonală cu blocuri a matricei

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

Matricea A o perceputem ca fiind matricea în baza standard a lui \mathbb{R}^5 a operatorului $T: \mathbb{R}^5 \rightarrow \mathbb{R}^5$, $T(x) = Ax$. Mai precis, dacă $x = (x_1, \dots, x_5)$, atunci $T(x_1, x_2, x_3, x_4, x_5) = (x_2 + x_3 + x_5, x_3 + x_4 + x_5, 0, 0, 0)$.

Aveam $A \neq 0$ și $A^3 = 0$, deci indicele de nilpotență este $r = 3$. Deoarece $\dim(\mathbb{R}^5) = \dim(\text{Im } T) + \dim(\ker T) = \text{rang}(A) + \dim(\ker T) \Rightarrow \dim(\ker T) = 3$, deci sunt trei blocuri H, dintre care unul de ordinul 3. Atunci, celelalte două sunt de ordinul 1, iar reprezentarea lui T ca matrice diag. cu blocuri este

$$\left(\begin{array}{ccccc|cc} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Forma canonică Jordan

Este o reprezentare matricială a opér. liniarii care are toate val. proprii în K, dar nu are o reprezentare diagonală devanscă pentru cel puțin o val. proprie λ_i , $\dim V_{\lambda_i} <$ multiplicitatea lui λ_i . Forma canonică Jordan este o matrice diagonală cu blocuri de forme

$$J_{ij} = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_i & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & & \lambda_i & 1 \\ 0 & 0 & 0 & & 0 & \lambda_i \end{pmatrix} \in M_j(K)$$

numite blocuri (sau celule) Jordan. Si observam că

$$\begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_i & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \lambda_i & 1 & 0 \\ 0 & 0 & 0 & 0 & \lambda_i & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_i \end{pmatrix} = \begin{pmatrix} \lambda_i & 0 & \dots & 0 & 0 \\ 0 & \lambda_i & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \lambda_i & 0 & 0 \\ 0 & 0 & 0 & \lambda_i & 0 \\ 0 & 0 & 0 & 0 & \lambda_i \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

deci

$$J_{ij} = \lambda_i I + H,$$

unde H este un bloc nilpotent care apare în cadrul op. nilpotenți.

Ac. descomp. a lui J_{ij} este, de fapt, consecința descompunerii op. $T: V \rightarrow V$ într-o sumă directă de operatori, fiecare sumand T_i fiind, la rândul său, suma dintre un op. scalar ($v \mapsto \lambda_i v$) și un op. nilpotent, ace cum rezultă din teorema următoare.

TEOR. 6. Fie $T: V \rightarrow V$ un op. liniar ale cărui polinoame caracteristice și minimal sunt respective

$$\Delta(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_n)^{m_n} \quad \text{și} \quad m(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_n)^{m_n},$$

unde λ_i sunt distincți. Atunci T are o reprezentare matricială diagno-

$$J_{ij} = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda_i & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda_i & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda_i \end{pmatrix} \in M_j(\mathbb{K}). \quad (4)$$

Pentru fiecare λ_i blocurile J_{ij} au următoarele proprietăți:

(i) Există cel puțin un bloc J_{i,m_i} de ordin m_i ; celelalte blocuri J_{ij} sunt de ordin $\leq m_i$.

(ii) Suma ordinelor blocurilor J_{ij} este m_i .

(iii) Numărul blocurilor J_{ij} este egal cu multiplicitatea geometrică a val. propriu λ_i (adică, egal cu $\dim_{\mathbb{K}} V_{\lambda_i}$)

(iv) Numărul blocurilor J_{ij} de fiecare ordin posibil este unic determinat de T .

Dem. Cf. Teor. 19/L5 de descompunere primară, $T = T_1 \oplus \dots \oplus T_r$ și $(\lambda - \lambda_i)^{m_i}$ este polinomul minimal al lui T_i . Atunci, $(T_i - \lambda_i I)^{m_i} = 0$, prin urmare op. $H_i := T_i - \lambda_i I$ este nilpotent de indice m_i . Asadar, T_i este o sumă

$$T_i = \lambda_i I + H_i$$

dintre op. scalari $\lambda_i I$ și op. nilpotent H_i . Folosind Teor. 4, op. N_i are o reprezentare matricială diagonală cu blocuri de forme (1). În raport cu baza care asigură ac. reprezentare a lui H_i , matricea M_i a lui $\lambda_i I + H_i$ are diag. principală al cărui se duc blocuri de forma (4). Mai departe, matricea M a lui T este suma directă

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_r.$$

Cu Prop. 8/L11, M are forma din enunțul teoremei.

Proprietățile (i) - (iv) sunt consecințe ale Teor. 4 deoarece forma matricii M_i este dată de op. nilpotent H_i . Astfel proprietatea (i) rezultă din faptul că H_i are indicele de nilpotență m_i (ver. Teor. 4). Proprietatea (ii) spune că matricea M_i are ordinul n_i ; întrucât rezultă din forma lui J rezultă că

$$\Delta_i(\lambda) = |\lambda I - J| = |\lambda I - M_1| \cdots |\lambda I - M_r|$$

Deoarece $|\lambda I - M_i| = (\lambda - \lambda_i)^{n_i} \Rightarrow M_i$ este de ordinul n_i . Prop. (iii) rezultă din Teor. 4, c.c. numărul blocurilor este egal cu $\dim(\text{Ker } H_i)$, iar $\text{Ker } H_i = V_{\lambda_i}$. În final, (iv) este o consecință a faptului că T_i și $\det H_i$ sunt unic determinați de T . ■

APLICAȚIA 6. Se determină toate formele canonice Jordan ale op. liniei $T: V \rightarrow V$ al cărui polinom caracteristic este $\Delta(\lambda) = (\lambda-4)^3(\lambda-7)^2$.

Forma Jordan este dată de opoziție de $\Delta(\lambda)$ și de polinomul minim $m(\lambda)$.

Astfel,

dacă $m(\lambda) = (\lambda-4)(\lambda-7)$, atunci $J = \begin{pmatrix} 4 & & & \\ & 4 & & \\ & & 4 & \\ & & & 7 \end{pmatrix};$

dacă $m(\lambda) = (\lambda-4)^2(\lambda-7)$, atunci $J = \begin{pmatrix} 4 & 1 & 0 & \\ 0 & 4 & & \\ & & 4 & \\ & & & 7 \end{pmatrix};$

dacă $m(\lambda) = (\lambda-4)^3(\lambda-7)$, atunci $J = \begin{pmatrix} 4 & 1 & 0 & \\ 0 & 4 & 1 & \\ 0 & 0 & 4 & \\ & & & 7 \end{pmatrix};$

dacă $m(\lambda) = (\lambda-4)(\lambda-7)^2$, atunci $J = \left(\begin{array}{c|cc} 4 & & \\ \hline & 4 & \\ & & 7 & 1 \\ & & 0 & 7 \end{array} \right)$;

dacă $m(\lambda) = (\lambda-4)^2(\lambda-7)^2$, atunci $J = \left(\begin{array}{c|cc} 4 & 1 & \\ \hline 0 & 4 & \\ \hline & 4 & \\ & & 7 & 1 \\ & & 0 & 7 \end{array} \right)$;

dacă $m(\lambda) = (\lambda-4)^3(\lambda-7)^2$, atunci $J = \left(\begin{array}{c|cc} 4 & 1 & 0 & \\ \hline 0 & 4 & 1 & \\ \hline 0 & 0 & 4 & \\ \hline & & & 7 & 1 \\ & & & 0 & 7 \end{array} \right)$;

APLICATIA 7. Găsești tracătate formule canonice Jordan ale unei matrice de ordinul 5 și cărei polinom minimal este $m(\lambda) = (\lambda-2)^2$

Aici, $\Delta(\lambda) = (\lambda-2)^5$ și $m(\lambda) = (\lambda-2)^2$. Atunci, J poate fi

$$J = \left(\begin{array}{c|cc} 2 & 1 & \\ \hline & 0 & 2 \\ & & \begin{array}{c|cc} 2 & 1 & \\ \hline 0 & 2 & \\ \hline & 2 & \end{array} \end{array} \right) \quad \text{ sau } J = \left(\begin{array}{c|cc} 2 & 1 & \\ \hline 0 & 2 & \\ \hline & 2 & \\ & & 2 \\ & & & 2 \end{array} \right)$$

OBS. Dacă polinomul caracteristic nu se descompune în factori liniali (adică, nu toate val. proprii se află în corpul K - de regulă $K = \mathbb{R}$), atunci există o formă canonica diagonală pe blocuri, numită formă canonica născătoare, în care celulele sunt matrice de forme

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & 0 & & 0 & -\alpha_1 \\ 0 & 1 & 0 & & 0 & -\alpha_2 \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & & 0 & -\alpha_{k-2} \\ 0 & 0 & 0 & & 1 & -\alpha_{k-1} \end{pmatrix}$$

Matricea C este numită matricea companion a unui polinom $m(\lambda) = d^k + a_{k-1}\lambda^{k-1} + \dots + a_1\lambda + a_0 \in K[\lambda]$.

APLICATIA 5'. Completam aplicatia 5 cu identificarea bazei lui \mathbb{R}^5 in raport cu care op. liniar $T: \mathbb{R}^5 \rightarrow \mathbb{R}^5$, $T(x_1, x_2, x_3, x_4, x_5) = (x_2 + x_3 + x_5, x_3 + x_4 + x_5, 0, 0, 0)$ are matricele

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

Ca baza este cea descrisă în demonstrație Teor. 4.

Ordinalul de nilpotență al lui T este 3. Cu not. $W_i := \text{Ker } T^i$ avem

$W_1 \subset W_2 \subset W_3 = \mathbb{R}^5$. și notăm $m_i := \dim_{\mathbb{R}} W_i$.

I Mai întâi căutăm o bază $B = \{u_1, u_2, \dots, u_m\}$ a \mathbb{R}^5 astfel încât $\{u_1, \dots, u_m\}$ să fie baza a lui W_1 .

$$(1) W_1 = \text{Ker } T = \{(x_i) \mid T(x_i) = 0\} = \{(x_1, x_2, x_3, x_4, x_5) \mid x_2 + x_3 + x_5 = 0, x_3 + x_4 + x_5 = 0\}.$$

Să găsim baza $\{u_1 = (1, 0, 0, 0), u_2 = (0, 1, -1, 1, 0), u_3 = (0, 0, -1, 0, 1)\}$, deoarece $m_1 = 3$

$$(2) W_2 = \text{Ker } T^2 = \{(x_i) \mid T^2(x_i) = 0\} = \{(x_1, x_2, x_3, x_4, x_5) \mid x_3 + x_4 + x_5 = 0\}; \dim W_2 = 4$$

Mai o bază a \mathbb{R}^4 să fie $\{u_1, u_2, u_3, u_4 = (0, 1, 0, 0, 0)\}$

$$(3) W_3 = \mathbb{R}^3 \text{ și o bază a sa este } \{u_1, u_2, u_3, u_4, u_5 = (0, 0, 0, 0, 1)\} = B$$

II C. dem. Teor. 4, vech. baza B se reprezintă astfel

$$B = \{u_1, u_2, u_3, w_1, w_1^3\}, \text{ unde } w_1^3 = u_5.$$

Multimea

$$S_1 = \{u_1, u_2, u_3, T(w_1^3)\} \subset W_2$$

este liniar independentă chiar și baza pt W_2 . Notăm $w_1^2 = T(w_1^3)$, deoarece $w_1^2 = T(0, 0, 0, 0, 1) = (1, 1, 0, 0, 0)$. Deoarece

$$S_1 = \{u_1, u_2, u_3, w_1^2\}.$$

Vom, $T(w_1^2) = w_1^1$ și introducem într-o bază a lui W_1 . Atenție $w_1^1 = T(w_1^2) = T(1, 1, 0, 0, 0) = (1, 0, 0, 0, 0)$. Vectorii baza în care matricele sunt formate de mai sus sunt prezintăți, cf. dem Teor. 4

$$w_1^3$$

$$w_1^2$$

$$w_1^1, w_2^1 = u_2, w_3^1 = u_3$$

$$\text{și sunt ordonati } (w_1^1, w_2^1, w_3^1, w_1^2, w_1^3) = B'$$

Să probăm afirmația că matricea $(T)_B'$ este cea de mai sus.

$$T(w_1^1) = T(1, 0, 0, 0, 0) = (0, 0, 0, 0, 0) = 0w_1^1 + 0w_2^1 + \dots + 0w_3^1$$

$$T(w_2^1) = T(1, 1, 0, 0, 0) = (1, 0, 0, 0, 0) = 1w_1^1 + 0w_2^1 + \dots + 0w_3^1$$

$$T(w_1^3) = T(0, 0, 0, 0, 1) = (1, 1, 0, 0, 0) = 0 \cdot w_1^1 + 1 \cdot w_1^2 + 0 \cdot w_1^3 + \dots + 0 \cdot w_3^1$$

$$T(w_2^1) = T(u_2) = (0, 0, 0, 0, 0) = 0 \cdot w_1^1 + 0 \cdot w_1^2 + \dots + 0 \cdot w_3^1$$

$$\text{and } T(w_3^1) = T(u_3) = (0, 0, 0, 0, 0) = 0 \cdot w_1^1 + 0 \cdot w_1^2 + \dots + 0 \cdot w_3^1$$

choose $u_2, u_3 \in \text{Ker } T$. In definitio,

$$(T)_{B'} = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

Ex. 1. Arătați că matricea

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & \dots & \dots & a_{1m-1} & a_{1m} \\ 0 & 0 & a_{23} & \dots & \dots & a_{2m-1} & a_{2m} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & & & 0 & a_{m-1,m} \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 \end{pmatrix} \quad (1)$$

este nilpotentă.

Ex. 2. Arătați că op. $T: \mathbb{R}^5 \rightarrow \mathbb{R}^5$, $T(x_1, x_2, x_3, x_4, x_5) = (x_2 + 2x_3 - x_4 - x_5, 3x_3 + x_4 + x_5, 0, -7x_5, 0)$ este nilpotent și găsiți indicele de nilpotență a lui T .

Ex. 6. Folosind Prop. 1/L12 găsiți un exemplu de subspațiu T -invariant.

Ex. 5. Arătați că $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $T(x, y, z) = (2x - 4y - 10z, 2y + 2z, x - y - 4z)$ este nilpotent.

Ex. 4. Arătați că dacă $P \in M_n(\mathbb{K})$ este inversabil și $A \in M_n(\mathbb{K})$ nilpotent, atunci $A_1 = P^{-1}AP$ este nilpotent. Aplicatie: fie

$$A = \begin{pmatrix} 0 & 2 & -3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad P = \begin{pmatrix} 3 & 1 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \quad \text{Determinați } T: \mathbb{R}^3 \rightarrow \mathbb{R}^3 \text{ op. liniar}$$

care în raport cu baza standard a lui \mathbb{R}^3 are matricea $A_1 = P^{-1}AP$.

Ex. 3. Arătați că op. elementare pe liniile și pe coloane transformă o matrice diagonală

$$D = \begin{pmatrix} d_1 & & \\ & d_2 & 0 \\ 0 & & d_n \end{pmatrix}$$

într-o matrice cu determin. egal cu $\det(D)$. Aplicatie: determinați o matrice cu toate elem. nemulte care sunt determin. egal cu 6.

Ex. 7. Determinați reprezentările matricale diagonale cu blocuri pt. op. de la Ex. 2 și Ex. 5.

Ex. 8. a) $T(x, y, z) = (2x + 2y + z, 2y - z, -x - 4y + 2z)$, $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$

(i) Arătați că $\Delta_T(\lambda) = (\lambda - 4)(\lambda - 1)^2$

(ii) Scrieți pe V ca o sumă directă $V = \text{Ker } g(T) \oplus \text{Ker } h(T)$ în sensul Lemiei 9/L11.

E9. ($T = T_1 \oplus T_2 \oplus \dots \oplus T_n$, Prop 8/11)

Fix $T: \mathbb{R}^4 \rightarrow \mathbb{R}^4$, $T(x, y, z, t) = (x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta, 3z - t, z + 2t)$

1) $W_1 = \{(x, y, 0, 0)\} \cong W_2 = \{(0, 0, z, t)\}$ subsp. T -invariant.

2) Do 9. Béton $W_i \ni A_i = (T_i)_{B_i}$, et

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Forma canonica Jordan
(exercitiu rezolvat)

Fie $T: \mathbb{R}^4 \rightarrow \mathbb{R}^4$ op. liniar definit prin

$$T(x, y, z, t) = (3x - y + z + t, -2x + 3y - 2z - t, -3x + y - 2z, -4x + y - z - 2t)$$

Să găsim forma canonica Jordană J a matricei lui T și o bază

Bază \mathbb{R}^4 a.i. $(T)_B = J$.

Sol.: În raport cu baza standard a lui \mathbb{R}^4 , matricea lui T este

$$A = \begin{pmatrix} 3 & -1 & 1 & 1 \\ -2 & 3 & -2 & -1 \\ -3 & 1 & -2 & 0 \\ -4 & 1 & -1 & -2 \end{pmatrix}$$

$$\Delta_T(\lambda) = \Delta_A(\lambda) = \det(\lambda I - A) = \begin{vmatrix} \lambda - 3 & 1 & -1 & -1 \\ 2 & \lambda - 3 & 2 & 1 \\ 3 & -1 & \lambda + 2 & 0 \\ 4 & -1 & 1 & \lambda + 2 \end{vmatrix} = (\lambda - 2)^2(\lambda + 1)^2$$

Valori proprii sunt $\lambda = 2$ și $\lambda = -1$, ambele multe de ordinul 2

Să găsim polinomul minimal $m_T(\lambda) = (\lambda - 2)^i(\lambda + 1)^j$, $1 \leq i, j \leq 2$.

$$A - 2I = \begin{pmatrix} 1 & -1 & 1 & 1 \\ -2 & 1 & -2 & -1 \\ -3 & 1 & -2 & 0 \\ -4 & 1 & -1 & -4 \end{pmatrix} \quad \text{și} \quad A + I = \begin{pmatrix} 4 & -1 & 1 & 1 \\ -2 & 4 & -2 & -1 \\ -3 & 1 & -1 & 0 \\ -4 & 1 & -1 & -1 \end{pmatrix}$$

Fie $(A - 2I)(A + I) = (b_{ij})$. Deoarece $b_{11} = -1 \neq 0 \Rightarrow m_T(\lambda) \neq (\lambda - 2)(\lambda + 1)$.

Verificăm dacă $m_T(\lambda) = (\lambda - 2)^2(\lambda + 1)$:

$$(A - 2I)^2 = \begin{pmatrix} 1 & -1 & 1 & 1 \\ -2 & 1 & -2 & -1 \\ -3 & 1 & -2 & 0 \\ -4 & 1 & -1 & -4 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 & 1 \\ -2 & 1 & -2 & -1 \\ -3 & 1 & -2 & 0 \\ -4 & 1 & -1 & -4 \end{pmatrix} = \begin{pmatrix} 4 & 0 & -2 & -2 \\ 6 & 0 & 5 & 1 \\ 7 & 0 & 11 & -4 \\ 13 & 0 & 2 & 11 \end{pmatrix}$$

Fie $(A - 2I)^2(A + I) = (c_{ij})$. Pt. c. $c_{11} = 30 \neq 0 \Rightarrow m_T(\lambda) \neq (\lambda - 2)^2(\lambda + 1)$.

Verificăm dacă $m_T(\lambda) = (\lambda - 2)(\lambda + 1)^2$:

$$(A + I)^2 = \begin{pmatrix} 4 & -1 & 1 & 1 \\ -2 & 4 & -2 & -1 \\ -3 & 1 & -1 & 0 \\ -4 & 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} 4 & -1 & 1 & 1 \\ -2 & 4 & -2 & -1 \\ -3 & 1 & -1 & 0 \\ -4 & 1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 11 & -6 & 4 & 4 \\ -6 & 15 & -7 & -5 \\ -11 & 6 & -4 & -4 \\ -11 & 6 & -4 & -4 \end{pmatrix}$$

Fie $(A - 2I)(A + I)^2 = (d_{ij})$. Deoarece $d_{11} = -5 \neq 0 \Rightarrow m_T(\lambda) = (\lambda - 2)(\lambda + 1)^2$.

In definitiv, $m_T(\lambda) = (A - 2I)(A + I)^2 = \Delta_T(\lambda)$.

PCB - 2/4

Rezultă că forma canonica Jordan este matricea

$$J = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

În continuare, ne propunem să găsim o bază B a lui \mathbb{R}^4 în raport cu care $(T)_{\mathbb{R}} = J_1$. Pentru aceasta vom folosi Teor. 18/L 5-8:

$$\mathbb{R}^4 = W_1 \oplus W_2,$$

unde $W_1 = \text{Ker}(T - 2I)^2$ este un subspace T-invariant și $f_1(\lambda) = (\lambda - 2)^2$ este polinomul minimal al lui $T_1 := T|_{W_1}$, iar $W_2 = \text{Ker}(T + I)^2$ este subspace T-invariant și $f_2(\lambda) = (\lambda + 1)^2$ este polinomul minimal al restricției $T_2 := T|_{W_2}$. În particular, $T = T_1 \oplus T_2$.

I) Să determinăm W_1 :

$$W_1 = \text{Ker}(T - 2I)^2 = \left\{ (x, y, z, t) \in \mathbb{R}^4 \mid (A - 2I)^2 \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 0 \right\}$$

$$\text{Ec. } (A - 2I)^2 \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 0. \text{ Înseamnă să se} \quad \begin{pmatrix} 4 & 0 & -2 & -2 \\ 6 & 0 & 5 & 1 \\ 7 & 0 & 11 & -4 \\ 13 & 0 & 2 & 11 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \quad (1)$$

Echivalent matricial:

$$\begin{pmatrix} -4 & 0 & -2 & -2 \\ 6 & 0 & 5 & 1 \\ 7 & 0 & 11 & -4 \\ 13 & 0 & 2 & 11 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 1 & 1 \\ 6 & 0 & 5 & 1 \\ 7 & 0 & 11 & -4 \\ 13 & 0 & 2 & 11 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 0 & 4 & -4 \\ 0 & 0 & 15 & -15 \\ 0 & 0 & -9 & 9 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Să se rezolve sistemul: } \begin{cases} 2x + 0 \cdot y + z + t = 0 \\ z - t = 0 \end{cases}$$

$\dim_{\mathbb{R}} W_1 = 2$ și o bază a sa se obține lărind:

$$\star y=1, t=0 \text{ de unde, } e_1 = (0, 1, 0, 0)$$

$$\star t=1, y=0 \text{ de unde } e_2 = (-1, 0, 1, 1).$$

Denumim $B_1 = \{e_1, e_2\}$ să fie o bază a lui W_1 .

Cine este $T_1 = T|_{W_1}$?

$$T_1(e_1) = T(0, 1, 0, 0) = (-1, 3, 1, 1) = (0, 3, 0, 0) + (-1, 0, 1, 1) = 3e_1 + e_2 \Rightarrow (T_1)_{B_1} = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$$

$$T_1(e_2) = T(-1, 0, 1, 1) = (-1, -1, 1, 1) = (0, -1, 0, 0) + (-1, 0, 1, 1) = -e_1 + e_2$$

$$w_1 = \alpha_1 e_1 + \alpha_2 e_2 \Rightarrow T(w_1) = \alpha_1 T(e_1) + \alpha_2 T(e_2) = \alpha_1 (3e_1 + e_2) + \alpha_2 (-e_1 + e_2) = (3\alpha_1 - \alpha_2) e_1 + (\alpha_1 + \alpha_2) e_2.$$

Problema: $m_{T_1}(\lambda) = (\lambda - 2)^2$:

$$(T_1)_{B_1} - 2I = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ deci } m_{T_1}(\lambda) = (\lambda - 2)^2.$$

Acum urmăru dem. Teor 6/L6-7 :

$(T_1 - 2 \text{Id}_{W_1})^2 = 0 \Rightarrow H_1 = T_1 - 2 \text{Id}_{W_1}$ este nilpotent de indice 2. Deci,

$$T_1 = 2 \text{Id}_{W_1} + H_1.$$

Mai departe, folosim Prop. 2/L6-2 : $H_1(e_1) = 0 \Rightarrow H_1(e_1) \neq 0 \Rightarrow$
 $S_1 = (H_1(e_1), e_1)$ este o bază ortonormală a lui W_1 în raport cu care

$$(H_1)_{S_1} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

$$\left[\begin{array}{l} \text{Intr-adevăr, } \begin{cases} H_1(H_1(e_1)) = T(T(e_1)) = 0 = 0 \cdot H_1(e_1) + 0 \cdot e_1, \\ H_1(e_1) \end{cases} \\ \Rightarrow (H_1)_{S_1} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{array} \right]$$

$$\text{Deci } (I_{W_1})_{S_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow (T_1)_{S_1} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

Incheiem cu menținerea $S_1 = (H_1(e_1), e_1) = (-1, 1, 1, 1), e_1 = (0, 1, 0, 0)$

II să determinăm W_2 :

$$W_2 = \text{Ker}(A+I)^2 = \left\{ (x, y, z, t) \in \mathbb{R}^4 \mid (A+I) \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 0 \right\}$$

$$(A+I)^2 = \begin{pmatrix} 11 & 6 & 4 & 4 \\ -6 & 15 & -7 & -5 \\ -11 & 6 & -4 & -4 \\ -11 & 6 & -4 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 11 & -6 & 4 & 4 \\ 6 & -15 & 7 & 5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} (11) & -6 & 4 & 4 \\ 0 & 129 & 53 & 31 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Sunt } \begin{cases} 11x = 6y + 4z + 4t = 0 \\ 129y = 53z + 31t = 0 \end{cases}$$

ne dă doi vectori ai bazei B_2 a lui W_2 : $f_1 = (-18, 53, 129, 0), f_2 = (-30, 31, 0, 129)$

Pentru $H_2 = T_2 + \text{Id}_{W_2}$ avem

$$H_2(f_1) = T_2(f_1) + f_1 = T(f_1) + f_1 = (22, -63, -151, -4) + (-18, 53, 129, 0) = (4, -10, -22, -4)$$

În raport cu baza $S_2 = (H_2(f_1), f_1)$ matricea lui T_2 este

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Asadar,

$$J = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

este matricea lui T cu baza ordonată

$$S = (S_1, S_2)$$

$$= ((-1, 1, 1, 1), (0, 1, 0, 0), (4, -10, -22, -4), (-18, 53, 123, 0))$$

Matr. de trunchie P de la baza standard a lui \mathbb{R}^4 la baza S
este

$$P = \begin{pmatrix} -1 & 0 & 4 & -18 \\ 1 & 1 & -10 & 53 \\ 1 & 0 & -22 & 123 \\ 1 & 0 & -4 & 0 \end{pmatrix}$$

Cititorul este invitat să probăcă relația

$$P^{-1}AP = J,$$

$$\text{echivalentă cu } AP = JP.$$

Inele

Că structură algebrică, inelul este un triplu $(R, +, \cdot)$ unde R este o multime nevidă, iar $+$ și \cdot sunt două op. numite generic adunare și înmulțire. Deși, perechea $(R, +)$ este un grup abelian, proprietățile evidențiate pt. grupuri nu sunt automat transferabile inelului. Elă tb. nu fie în concordanță cu op. de înmulțire, op. în raport cu care pot fi situații dintr-o cale mai diverse: pot exista elemente nerule ale căror produs este zero, pot exista elemente nerule ce au puteri nule, pot exista elemente care nu sunt inverseabile etc. Relația de echivalență pe un inel este, de asemenea, una mai complexă. Subinelul nu are proprietăți suficiente pentru a defini o rel de echivalență, astă cum subgrupul îndefineste orelă între-un grup. Este nevoie de o submultime cu o proprietate mai "tare" pentru op. de înmulțire, numită ideal.

1. Inele și morfisme de inele

(1.1) DEF. Un inel este o multime nevidă R împreună cu două operații binare, ușor notate aditivă (adică, cu $+$) și multiplicativă (adică, cu \cdot), a. z.

- (a) $(R, +)$ este un grup abelian;
- (b) $(ab)c = a(bc)$, $\forall a, b, c \in R$ (adică, înmulțirea este asociativă)
- (c) $a(b+c) = ab+ac$ și $(a+b)c = ac+bc$ (înmulțirea este distributivă față de adunare).

Dacă, în plus:

- (d) R conține un element 1 a. z.

$$1 \cdot a = a \cdot 1 = a, \quad \forall a \in R,$$

at. R s.m. inel cu unitate sau unitar. În fine, R este inel comutativ dacă $ab = ba$, $\forall a, b \in R$.

Căteva proprietăți imediate într-un inel sunt date mai jos.

(1.2) PROP. Într-un inel R au loc relațiile:

- (i) $0 \cdot a = a \cdot 0 = 0, \quad \forall a \in R;$
- (ii) $(-a)b = a(-b) = - (a \cdot b), \quad \forall a, b \in R;$
- (iii) $(-a)(-b) = ab, \quad \forall a, b \in R;$

(iv) $(ma)b = a(mb) \cdot m(ab)$, $\forall m \in \mathbb{Z}$ și $\forall a, b \in R$, unde am notat

$$ma = \begin{cases} a + a + \dots + a & (\text{m sumanți}), \text{ dacă } m > 0 \\ (-a) + (-a) + \dots + (-a) & (-m \text{ sumanți}), \text{ dacă } m < 0 \end{cases}$$

$$(v) \left(\sum_{i=1}^m a_i \right) \left(\sum_{j=1}^n b_j \right) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j, \quad \forall a_i, b_j \in R$$

Dem. (schite) (i) $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$, $-(0 \cdot a) + (0 \cdot a) = -(0a) + 0 \cdot a + 0 \cdot a$, deci $0 = 0 \cdot a$.
(ii) $ab + (-a)b = (a + (-a)) \cdot b = 0 \cdot b = 0$, de unde $(-a)b = -(ab)$. (iii) rezultă din (ii). Rel. (v) se dem. prin inducție, iar (iv) este un caz particular al lui (v). ■

In continuare, extindem terminologia.

(1.3) DEF. Un element nenul a din inelul R este un divizor la stg. (resp., la dr.) al lui zero dacă există $b \in R$ s.t. $a \cdot b = 0$ (resp., $b \cdot a = 0$). Elemt. a este, pun să simbolizăm, divizor al lui zero al lui R dacă este deopotrivă divizor la stg și la dr. al lui zero.

Cititorul poate arăta că în inelul R nu există divizori ai lui zero d.s.m.
în R se poate efectua simplificarea, adică pt. toti $a, b, c \in R$ cu $a \neq 0$,
 $ab = ac$ sau $ba = ca \Rightarrow b = c$.

(1.4) DEF. Un element a din inelul unitar R s.m. inversabil la stg. (resp., la dr.) dacă există $c \in R$ (resp., $b \in R$) s.t. $ca = 1$ (resp., $ab = 1$). Elemt. c (resp., b) s.m. invers la stg. (resp., la dr.) al lui a . Un element $a \in R$ care este deopotrivă inversabil la stg. și la dr. s.m. inversabil sau unitate.

(1.5) OBS(i) Dacă $a \in R$ este inversabil și la stg. și la dr., atunci elementele invers la stg. și la dr. coincid. Într-adevăr, din $ab = 1 = ca$ rezultă $b = 1 \cdot b = (ca)b = c(ab) = c = 1$.

(ii) Elemt. inversabile ale unui inel unitar formează un grup în raport cu înmulțirea, numit grupul unităților, notat $U(R)$.

(1.6) DEF. Un domeniu de integritate este un inel comutativ unitar cu $1 \neq 0$ și fără divizori ai lui zero. Un inel unitar ^{sau inel integral sau pm n. de grup, domeniu} în care orice element nenul ^{cu 1 ≠ 0}

De ex., în mulțimea $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}_2 \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{Z} \text{ și } b \in \mathbb{Z}_2 \right\}$, elem.

$a = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ este divizor de dr. al lui zero deoarece

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0$$

dacă a nu este divizor de dr. al lui zero deoarece condiție

$$\begin{pmatrix} x & \hat{y} \\ 0 & z \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

rezultă

$$\begin{pmatrix} 2x & \hat{y} \\ 0 & z \end{pmatrix} = 0,$$

rezp. $x=2=0$ și $\hat{y}=0$. Pe de altă parte, dacă $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, atunci $b^2 = 0$, ceea ce înseamnă că b este deosebit de divizor de dr. al lui zero. (verifică de exemplu)

este inversabil s.n. corp. Un corp comutativ sau camp este un corp în care înmulțirea este comutativă.

(1.7) OBS. (i) Un inel unitar este corp $\Leftrightarrow U(R) = \mathbb{R}^*$. (ii) Orice corp este un domeniu de integritate (anti-aderență), deci $a \cdot b = 0 \Rightarrow a \neq 0$, și $a^{-1}(ab) = 0 \Rightarrow b = 0$.

(1.8) EXEMPLU. Inelul \mathbb{Z} al întregilor este integru. Multimea $2\mathbb{Z}$ al întregilor pari este un inel integru fără unitate. Multimile \mathbb{Q} , \mathbb{R} , \mathbb{C} sunt corpuri comutative în raport cu oper. obișnuite de adunare și înmulțire. Mult. $M_n(K)$, unde $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ este un inel unitar necomutativ.

(1.8) EXEMPLU. Pentru fiecare întreg $n > 0$, multimea \mathbb{Z}_n a întregilor modul n este un inel. Dacă n nu e prim, și $n = kr$ cu $k > 1$, $r > 1$, atunci $\bar{k} \neq 0$, $\bar{n} \neq 0$ și $\bar{k} \cdot \bar{n} = \bar{k}r = \bar{r} = \bar{0}$ în \mathbb{Z}_n . Prin urmare, dacă n nu este prim, atunci în \mathbb{Z}_n există divizori ai lui zero.

(1.9) PROB. Dacă p este un nr. prim, atunci \mathbb{Z}_p este un corp (comutativ).

Dem. Fie $\bar{k} \in \mathbb{Z}_p^*$ și fie $k \in \mathbb{Z}$, unde $1 \leq k \leq p$. Dacă $(k, p) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ s.t. $ka + pb = 1$. Rezultă $\bar{k} \cdot \bar{a} = 1$, deci \bar{k} inversabil în \mathbb{Z}_p . ■

(1.10) EXEMPLU. Fie G un grup și fie $\text{End } G$ mulțimea endomorfismelor $f: G \rightarrow G$. Dacă $f, g \in \text{End } G$, atunci definim

$$(f+g)(x) := f(x) + g(x)$$

și

$$(fg)(x) = (f \circ g)(x),$$

unde „ \circ ” este compunerea funcțiilor. Cu aceste operații, $\text{End } G$ este un inel unitar, în general, necomutativ.

(1.11) EXEMPLU. Fie $H \subset M_2(\mathbb{C})$ mult. matricelor cu elem. de forma

$$q = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \quad \text{unde } a, b, c, d \in \mathbb{R}$$

$$\text{Notam: } i := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad i^2 := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ și } k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \text{ atunci}$$

$q \in H$ se poate scrie $q = a_1 + b_i + c_j + d_k$. Calculati $i^2, j^2, k^2, ij, ji, jk, kj, ti$, tk . Si arata: $\exists H$ este un grup noncomutativ. Acest inel s. n. corful quaternionilor.

→ morfism

(1.13) EXEMPLU (inelul semigroup). Sa si G este semigroup si R este un inel, iar $x_1, x_2, \dots, x_n \in G$ si $r_1, r_2, \dots, r_n \in R$, atunci vom avea expresii

$$r_1x_1 + r_2x_2 + \dots + r_nx_n$$

(i) Vom pomeni de la cazul particular al inelului de polinoame. Înmulțirea expresiilor cu coef. reale,

$$E(x) = a_0 + a_1x + \dots + a_{200}x^{200}$$

$$F(x) = b_0 + b_1x + \dots + b_{300}x^{300},$$

sugereaza, după cum vom vedea, abordarea notiunii de polinom. Din lucru cu expresii avem

$$E(x) \cdot F(x) = c_0 + c_1x + c_2x^2 + \dots + c_{500}x^{500},$$

unde $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$. Coeficientul c_k se obtine din simbol de egalitate

$$x^k = x^0 x^k = x^0 x^{k-1} = \dots = x^k x^0,$$

din care rezulta $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0 = \sum_{i+j=k} a_i b_{k-i}$. Observam că prezentă lini x este numai un auxiliar, deoarece putem privi produsul $E(x) \cdot F(x)$ în următorul cadrin simplificat:

$$E = (a_0, a_1, a_2, \dots), \quad a_i = 0 \text{ pt } i > 200,$$

$$F = (b_0, b_1, b_2, \dots), \quad b_j = 0 \text{ pt } j > 300,$$

și

$$EF = (c_0, c_1, c_2, \dots), \text{ unde } c_k = \sum_{i+j=k} a_i b_j.$$

Mai abstract, E și F sunt funcții definite pe \mathbb{N} , nule aproape peste tot, în sensul că suportul lor $\text{Supp}(E) = \{n \in \mathbb{N} \mid E(n) \neq 0\}$ și $\text{Supp}(F) = \{n \in \mathbb{N} \mid F(n) \neq 0\}$ sunt finite.

(ii) În lumina acestor considerații, un polinom cu coeficienți în inelul R este o funcție $f: \mathbb{N} \rightarrow R$ nulă a.p.t., în sensul că suportul său

$\text{Supp}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}$ este finit. Multimea $R^{(\mathbb{N})}$ a tuturor funcțiilor $f: \mathbb{N} \rightarrow R$ care sunt nule a.p.t. este un subgrup al grupului aditiv $R^{\mathbb{N}}$ în raport cu adunarea $f+g$ date prin $(f+g)(n) = f(n) + g(n)$. Deoarece

$\text{Supp}(f+g) \subseteq \text{Supp}(f) \cup \text{Supp}(g)$. Mai concret, dacă

$$f = (a_0, a_1, a_2, \dots) \text{ și } g = (b_0, b_1, b_2, \dots),$$

at.

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

(1.12) DEF. Fieind date două mulțimi R și S , și funcție $f: R \rightarrow S$ s.a. n. morfism (sau omomorfism) de unde dacă îndefineste următoarele două proprietăți :

- (i) $f(a+b) = f(a) + f(b)$, $\forall a, b \in R$;
- (ii) $f(ab) = f(a)f(b)$, $\forall a, b \in R$,

Prima proprietate exprimă faptul că f este un morfism de la grupul aditiv R la grupul aditiv S , de unde $f(0) = 0$ și $f(-a) = -f(a)$.

A doua proprietate nu conduce la relația $f(1_R) = 1_S$. De exemplu, aplicația $f: \mathbb{Z}_3 \longrightarrow \mathbb{Z}_6$, $f(\bar{k}) = \bar{4k}$ ($f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{4}$, $f(\bar{2}) = \bar{8}$) este un morfism cu $f(\bar{1}) \neq \bar{1}$. Un morfism de unde $f: R \rightarrow S$ cu proprietatea $f(1) = 1$ s.a. morfism unitar.

L1-1

unde am notat $a_n := f(n)$, $b_n := g(n)$, $\forall n \in \mathbb{N}$. Produsul $f \cdot g$ se definește prin

$$f \cdot g = (c_0, c_1, \dots), \quad \text{unde } c_k = \sum_{i+j=k} a_i b_j,$$

altfel spus, $f \cdot g : \mathbb{N} \rightarrow \mathbb{R}$ este familie de tipuri de perechi.

$$(f \cdot g)(k) := \sum_{i+j=k} f(i)g(j).$$

Mai departe, cu identificările

$$(0, 0, 0, \dots) = 0 \quad \text{și } (0, 1, 0, \dots) = X,$$

polinomul f se scrie

$$f = a_0 + a_1 X + a_2 X^2 + \dots,$$

dacă $\exists n \geq 0$ s.a.t. $a_m = 0$ și totuși $m > n$.

(ii) Acum, generalizăm construcția de la (ii) considerând că G este un semigrup multiplicativ cu unitate τ și R un anel. Pentru fiecare $f, g \in R^{(G)}$ definim $f+g \in R^{(G)}$ prin

$$(f+g)(x) = f(x) + g(x), \quad \forall x \in G \quad (1)$$

și definim produsul $f \cdot g$ prin

$$(f \cdot g)(x) = \sum_{y \in G} f(y)g(\tau(y)), \quad \forall x \in G. \quad (2)$$

(1) Arătăți că $R^{(G)}$ este un anel în raport cu operațiile (1) și (2). Aghjunctia $\{\tau\} : x \mapsto \tau(x)$ este unitate în $R^{(G)}$. Această anel s.n. inelul semigrupului (ori inelul grupului, dacă G este grup) al lui G peste R .

(2) Pentru fiecare $r \in R$ și fiecare $x \in G$ definim $\sigma(r)$ și $\tau(x)$ din $R^{(G)}$ prin

$$\sigma(r)(x) = \tau_{ex} r \quad \text{și } \tau(x)(y) = \tau_{xy}.$$

Arătăți că $\sigma : r \mapsto \sigma(r)$ definește un morfism injectiv de inele $R \rightarrow R^{(G)}$, iar $\tau : x \mapsto \tau(x)$ definește un morfism injectiv de monoz: $G \rightarrow R^{(G)}$ în semigrupul multiplicativ al lui $R^{(G)}$.

(3) Arătăți că pentru fiecare element nenul $f \in R^{(G)}$ există un sau unic r_0, r_1, \dots, r_n de elemente nenule din R și de elemente distincte $x_1, \dots, x_n \in G$ a.s.

$$f = \sigma(r_1)\tau(x_1) + \sigma(r_2)\tau(x_2) + \dots + \sigma(r_n)\tau(x_n).$$

Dovărește că și τ sunt injectii, cu identificările $\sigma(r_i) = r_i$ și $\tau(x_i) = x_i$, elem. f se scrie, pur și simplu

$$f = r_1 x_1 + r_2 x_2 + \dots + r_n x_n.$$

Să observăm că în acestă notatie imaginae consoñă a lui $r \in R$ în $R^{(G)}$

prin morfismul σ este re, unitatea din $R^{(G)}$ este re și

$$(r_1x_1 + \dots + r_nx_n)(s_1y_1 + \dots + s_my_m) = \sum_{i,j \in I} r_i s_j x_i y_j.$$

(4) Fie S un inel și fie $\varphi: R \rightarrow S$ un morfism de inele, iar $\Theta: G \rightarrow S$ un morfism de monozice la semigrupul multiplicativ al lui S a.s. $\varphi(r)\Theta(x) = \Theta(x)\varphi(r)$, $\forall r \in R, \forall x \in G$. Arătăți că există un unic morfism de inele $\Psi: R^{(G)} \rightarrow S$ a.s. $\Psi \circ \sigma = \varphi$ și $\Psi \circ \theta = \Theta$, adică Ψ face comutativ diagramile de mai jos,

$$\begin{array}{ccc} R & \xrightarrow{\sigma} & R^{(G)} \\ \downarrow \varphi & & \downarrow \Psi \\ S & & \end{array} \quad \begin{array}{ccc} G & \xrightarrow{\theta} & R^{(G)} \\ \downarrow \Theta & & \downarrow \Psi \\ S & & \end{array}$$

în dubla calitate de morfism de inele și de morfism de semigrupuri.

Un monomorfism (resp. epimorfism, izomorfism) de inele este un morfism de inele care este și aplicatie injectivă (resp. surjectivă, bijectivă). Un monomorfism $R \rightarrow S$ este numit, uneori, surfundare (sau incarcare) a lui R în S .

Dacă $f: R \rightarrow S$ este morfism de inele, at $\text{Ker } f = \{r \in R | f(r) = 0\}$ și $\text{Im } f = \{f(r) | r \in R\}$.

(1.14) EXEMPLU. Aplicația canonică $\mathbb{Z} \rightarrow \mathbb{Z}_n$, date prin $k \mapsto \hat{k}$ este un epimorfism de inele. Aplicația $\mathbb{Z}_4 \rightarrow \mathbb{Z}_8$, date prin $\hat{k} \mapsto \overline{2k}$ este un monomorfism.

(1.15) PROP. Orice inel R poate fi surfundat într-un inel cu unitate S .

DIM. Fie $S = R \oplus \mathbb{Z}$, sumă directă de grupuri comutative. Pe S definim înmulțirea prin

$$(r_1, m_1) \cdot (r_2, m_2) := (r_1 r_2 + m_1 r_2 + m_2 r_1, m_1 m_2).$$

Atunci S este inel cu unitatea $(0, 1)$. Aplicația $R \rightarrow S$ date prin $r \mapsto (r, 0)$ este și surfundare a lui R în S .

EXERCITII

- Fie G un grup (adiciv) abelian. Definim $a \cdot b = 0$, $\forall a, b \in G$. Atunci G este inel.
- Fie $R = \mathcal{P}(T)$, unde T este o mulțime nevoid. Pentru $A, B \in R$ definim

$$A + B = (A \setminus B) \cup (B \setminus A) \quad \text{și} \quad AB = A \cap B.$$

Arătăți că R este un inel comutativ unitar.

- Fie $\{R_i | i \in I\}$ o familie de inele unitare și fie $\sum_{i \in I} R_i = \{(r_i)_{i \in I} | r_i = 0 \text{ a.p.t. } i \in I\}$.

Arătăți că $\sum_{i \in I} R_i$ este un inel unitar împreună cu operațiile de adunare și înmulțire pe componente.

4. Un inel R cu $a^2 = a$, $\forall a \in R$ este numit inel boolean. Arătăți că orice inel boolean este comutativ și că $a \cdot a = 0$, $\forall a \in R$.

5. Dacă $G = \mathbb{Z}_2$ în Exemplul 1.10, atunci inelul $\text{End } G$ este comutativ.

6. Deoarece $G = \mathbb{Z} \oplus \mathbb{Z}$, atunci $\text{End } G$ este inel necomutativ. (Int. Se pot lua $f(m \oplus n) = (m+n) \oplus n$ și $g(m \oplus n) = m \oplus (m+n)$).

7. Fie $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}_2 \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, z \in \mathbb{Z} \text{ și } y \in \mathbb{Z}_2 \right\}$ împreună cu adunarea și

mărirea matricelor cu convenția $a \cdot \hat{b} := \hat{ab}$, $\forall a \in \mathbb{Z}$ și $\hat{b} \in \mathbb{Z}_2$. Deoarece

$$a = \begin{pmatrix} 2 & \hat{0} \\ 0 & 1 \end{pmatrix} \text{ și } b = \begin{pmatrix} 0 & \hat{1} \\ 0 & 0 \end{pmatrix},$$

(i) a este divizor la stg. al lui 0 , dacă nu e divizor la dr. al lui 0 .

(ii) b este un divizor al lui 0 , atât la stg. cât și la dr.

8. Fie R un inel cu cel puțin două elemente $a, b \in R$ și fiecare $a \neq 0$ din R ex.

șă existe unic număr $n \in \mathbb{N}$, $aba = a$. Arătăți că:

- (a) R nu are divizori ei lui zero;
- (b) $bab = b$;
- (c) R are unitate;
- (d) R este wcp.

Sol. (a) Este r_ef. să arătăm că dacă $a \neq 0$, atunci $ax = ay \Rightarrow x = y$. Din $ax = ay$ rezultă $ax - ay = 0$, $a(x - y) = 0$, respectiv $a(x - y)a = a - aba$, sau $a(x - y + b) = a$.

Astăzi $x - y + b = b$, deci $x = y$.

(b) $aba = a \Rightarrow abab = ab \Rightarrow a(bab - b) = 0 \xrightarrow{a \neq 0} bab = b$.

(c). Tb. să arătăm că $\exists c \in R$ s.t. $ac = ca = a$, $\forall a \in R$. Fie $a, c \in R$ și fie d pt. care $cd = c$. Dacă $aba = a \quad \left\{ \begin{array}{l} abac = ac \\ cdac = ac \end{array} \right. \Rightarrow a(ba - cd)c = 0 \Rightarrow ba = cd$. Astăzi, că mult.

$\{ab \mid a \in R\} \cap \{ba = a\}$ are un unic element, pe care să îl notăm cu e .

Astăzi $aba = a \Rightarrow ea = a$. Apoi, $a(ba - eb)a = 0 \Rightarrow ba = eb$, de unde $ba = e$ și $eba = a \Rightarrow ae = a$.

(c) $aba = a \quad \left\{ \begin{array}{l} a \neq 0 \Rightarrow (ab - 1)a = 0 \Rightarrow ab = 1 \\ \text{analog, } ba = 1 \end{array} \right. \text{ deci } b \text{ e inversul}$

2. Hol. de ideal

Fie R un inel și fie $S \subseteq R$ o submultime nevoidă care este parte stabilită în raport cu op. de adunare și înmulțire din R . Dacă S împreună cu cele două operații este un inel, atunci S este un subinel al lui R .

(2.1) EXEMPLE. \mathbb{Z} este un subinel al inelului \mathbb{Q} al nr. rationale. Multimea matricelor patrate de ordinul doi sau superior triunghiulare este un subinel al inelului $M_2(\mathbb{R})$ împreună cu op. obișnuite de adunare și înmulțire a matricelor.

Rostul idealelor într-un inel este similar subiectului într-un grup, anume îndeplinește rolul unui criteriu de clasificare a elementelor inelului și, mai mult decât atât, permite efectuarea de operații între clasele rezultate din clasificare. Astfel, fie R inel și fie $I \subseteq R$ un subgrup al grupului aditiv abelian $(R, +)$. Criteriul de clasificare al lui I se manifestă prin relația de echivalență modulo I ,

$$x \equiv y \pmod{I} \text{ dacă } x-y \in I.$$

Rezultatul „clasificării” sunt clasele de echivalență $a+I$, unde $a \in R$, notează și \bar{a} . Multimea cl. de echivalență se notează R/I sau $\frac{R}{I}$ și se mai numește multimea cat sau multimea factor a lui R prin I . Proprietățile lui I ne permit să definim o adunare pe multimea R/I :

$$(a+I) + (b+I) := (a+b) + I, \quad \forall a, b \in R. \quad (1)$$

Pentru definiția (1), R/I capătă o strucție de grup comutativ în care elementul zero este $\bar{0} = I$. Ce trebuie să stimăm ca să putem să adădă I pentru o operație de înmulțire naturală între clase,

$$(a+I) \cdot (b+I) := ab + I, \quad \text{unde } a, b \in R, \quad (2)$$

de să aibă sens? Din rel. (2) se observă că doar cerințele obligatorii sunt $aI \subseteq I$ și $Ib \subseteq I$, $\forall a, b \in R$. Pentru aceste motive se ajunge la definiția următoare.

(2.2) DEF. Un ideal în inelul R este o submultime nevoidă $I \subseteq R$ a. z. :

- (a) $x-y \in I$, $\forall x, y \in I$ (I este un subgrup al grupului aditiv R);
- (b) $rI \subseteq I$ și $Ir \subseteq I$, $\forall r \in R$ (I are proprietatea de absorbție).

În legătură cu împărțirea în clase de echivalență modulu I a elementelor inclusiui R vomintim \mathcal{I} :

$$(a) R/I = \{a+I \mid a \in R\};$$

$$(b) \bigcup_{a \in R} \{a+I\} = R.$$

La (b), R nu este o reuniune de submultimi disjuncte. Legătura este:

$$(c) \forall a, b \in R \text{ avem } SAV a+I = b+I \text{ (cind } a-b \in I, \text{ ori, echivalent, } a \equiv b \pmod{I})$$

$$SAV(a+I) \cap (b+I) = \emptyset \text{ (cind, } a-b \notin I \text{ ori, echivalent, } a \not\equiv b \pmod{I}).$$

(d) Dată că identificarea multimi factor R/I, următoarea provocare este de cărui o operatie ~~sarcine~~^{*}, ~~definită~~ între elementele inclusiui, poste fi metamorfozată într-o operatie între clase. De cărui $\hat{a}, \hat{b} \in R/I$ sunt clase, atunci ~~ca definitia~~

$$\hat{a} * \hat{b} := \overline{a+b}, \text{ unde } a \in \hat{a} \text{ și } b \in \hat{b} \quad (x)$$

ne dă o operatie între clase (se spune că defin. este bună) de cărui

$$\widehat{\hat{a} * \hat{b}} = \hat{a} * \hat{b}, \quad (xx)$$

oricare ar fi $a', a \in \hat{a}$ și $b', b \in \hat{b}$.

Practic, definitia (x) este una "bună" de cărui are loc implicativă: $a \equiv a \pmod{I} \wedge b \equiv b \pmod{I} \Rightarrow a' * b' \equiv a * b \pmod{I}$.

Implicativă de mai sus ne spune că "o definire bună" ^{între clase} înseamnă o definire care nu depinde de reprezentanții claselor.

EXEMPLU. $R = \mathbb{Z}$ și $I = 6\mathbb{Z}$. Identifică $\widehat{247}$, $\widehat{-335}$

EXEMPLU. $R = R[x]$ și $I = \langle x^2 + 1 \rangle$. Identifică $\widehat{x^3 + 1}$, $\widehat{3x^2 - 5}$.

EXERCITIU. Identifică elementele inclusiui factor $R/\langle 0 \rangle$ și deduciți că $R/\langle 0 \rangle \not\cong R$, deși izomorfismul $R/\langle 0 \rangle \cong R$ permite identificarea elementelor celor două inclusiui.

Dacă în locul condiției (b) are loc numai inclusiunea $rI \subseteq I$, atunci spunem că I este un ideal la stg., iar dacă are loc numai inclusiunea $Ir \subseteq I$, atunci spunem că I este un ideal la dr. Față de aceste precizări, def. 2.2 spune că un ideal este deopotrivă ideal la stg. și ideal la dr. (el fiind opus, ideal bilateral). Într-un inel comutativ toate ideile sunt bilaterale.

(2.3) EXEMPLU. Idealele inclusului \mathbb{Z} și întregitor sunt de forma $I = n\mathbb{Z}$, unde n este un întreg ≥ 0 .

(2.4) EXEMPLU. Fie R un inel comutativ și $a \in R$ un element fixat. Atunci, $I = aR$ este un ideal în R , notat adesea $\langle a \rangle$ și numit idealul generat de a .

(2.5) EXEMPLU. Fie R un inel unitar și $I \subseteq R$ un ideal. Atunci, $I = R \iff I = \langle 1 \rangle$.

(2.6) EXEMPLU. Fie R un inel și $C = C(R) = \{r \in R \mid rx = xr, \forall x \in R\}$ centralul lui R .

(i) $C \subseteq R$ este subinel al inclusului R ;

(ii) Dacă $R = M_2(\mathbb{R})$, atunci $C = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}$, și C nu este ideal.

(2.7) EXEMPLU. Dacă $f: R \rightarrow S$ este un morfism de inele, atunci $\text{Ker } f \subseteq R$ este un ideal, iar $\text{Im } f \subseteq S$ este un subinel.

Vom încheia acest paragraf dovedind că înmulțirea (2) determină strucțura de inel pe grupul aditiv R/I .

(2.8) TEOR. Fie R un inel și fie $I \subseteq R$ un ideal. Atunci grupul aditiv factor R/I este un inel cu înmulțirea definită prin

$$\xleftarrow{\quad} (a+I) \cdot (b+I) := ab + I.$$

Dacă R este comutativ sau are unitate, atunci tot așa este și R/I .

DEM. Este suficient să arătăm că înmulțirea este bine definită, căci proprietățile din defin. inclusului pot fi probate imediat. Astăzi, tb. că arătăm că dacă $a' \equiv a \pmod{I}$ și $b' \equiv b \pmod{I}$, atunci $a'b' \equiv ab \pmod{I}$. Din $a' \equiv a \pmod{I}$ rezultă că $a' - a \in I$, respectiv $a' - a = i$, $i \in I$, ori $a' = a + i$. Analog, $b' = b + j$, $j \in I$. Atunci $a'b' = (a+i)(b+j) = ab + aj + ib + ij$ și $a'b' - ab = aj + ib + ij$. I fiind ideal,

$\{ab+az \mid z \in I\}$ is a set of all linear combinations of a and b .

It is a subset of I . (Because $z \in I$ implies $az \in I$ and $ab \in I$)

It is a subset of I . (Because $z \in I$ implies $az \in I$ and $ab \in I$)

Thus $\{ab+az \mid z \in I\}$ is a subset of I .

$$\textcircled{*} \quad \{ab+az \mid z \in I\} = \{ab+zb \mid z \in I\}$$

este clar că $a'b' - ab \in I$, astfel că $a'b' \equiv ab \pmod{I}$ sau $a'b' + I = ab + I$. \blacksquare

3. Proprietăți ale idealului. Oper. cu ideale

(3.1) PROP. Fie $\{J_i\}_{i \in I}$ o familie de ideale bilaterale (le stg, le dr.) din inelul R .

Amenajării este un ideal bilateral (le stg, le dr.) în R .

(3.2) OBS. O reuniune de ideale nu este, în general, un ideal. Astfel, dacă suntem idealele lui \mathbb{Z} , $I = 2\mathbb{Z}$ și $J = 3\mathbb{Z}$, atunci $I \cup J = 2\mathbb{Z} \cup 3\mathbb{Z}$. Pe de o parte, $1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Pe de altă parte, dacă $I \cup J$ ar fi ideal, atunci $1 = 2 \cdot 5 + 3(-3) \in I \cup J$, contradicție.

(3.3) Fie R un inel și $X \subseteq R$ o submultime. Prin idealul bilaterial (le stg, le dr.) generat de multimea X se înțelege intersecția tuturor idealelor bilaterale (le stg, le dr.) care conțin pe X . Acest ideal se notează $\langle X \rangle_{\text{van}}(X)$, iar elementele mult. X sunt generatori. Dacă X este multime finită, $X = \{x_1, \dots, x_n\}$ atunci se spune că $\langle X \rangle$ este finit generat sau de tip finit și se scrie $\langle x_1, \dots, x_n \rangle$; este idealul generat de un singur element s.n. principal.

$X \subseteq R$ o submultime

(3.4) PROP (caracterizarea idealelor generate). Fie R un inel, $\forall_{\forall I \subseteq R}$ un ideal bilaterial (stg, dr.) din R . Atunci, următoarele afirmații sunt echivalente:

- (a) I este generat de multimea X ;
- (b) $I \supseteq X$ și pt. orice ideal bilaterial (stg., dr.) $J \supseteq X$ din R avem $J \supseteq I$; altfel,
- (c) I este multimea tuturor sumelor finite de forma

$$x = \sum r_i x_i + \sum s_j s_j + \sum m_k x_k + \sum n_m x_m s_m, \quad (3)$$

unde x -urile sunt din X , r_i -urile și s_j -urile sunt din R , m -urile sunt din \mathbb{Z} (n.r.p., $x = \sum r_i x_i + \sum m_k x_k$ și $x = \sum s_j s_j + \sum n_m x_m$).

Dem. (a) echiv. cu (b) deoarece orice intersecție de multimi este inclusă în oricare dintre multimiile intersecției.

(b) \Rightarrow (c). Notăm I' mult. elem de forma (3). I' verif. cond. din defin. idealului, deci I' este ideal. În plus, $I' \supseteq X$. Ambele ideale I și I' verifică ipoteza (b), prin urmare, $I \supseteq I'$ și $I \supseteq I'$, deci $I = I'$.

(c) \Rightarrow (b). Este clar că $I \supseteq X$. Deoarece idealul $J \supseteq X$, atunci J conține toate combinații de formă (3). Dar acesta înseamnă că $J \supseteq I$. \blacksquare

În acest lucru, să luăm în considerare că \mathcal{I} este un ideal generat de multe variabile. Dacă I este un ideal generat de o singură variabilă, atunci I^m este un ideal generat de monomii de gradul m . În acest caz, I^m este un ideal principal.

În general, I^m nu este un ideal principal. De exemplu, dacă $I = (x)$, atunci $I^m = (x^m)$ este un ideal principal. Dar dacă $I = (x_1, x_2, \dots, x_n)$, atunci $I^m = (x_1^m, x_2^m, \dots, x_n^m)$ nu este un ideal principal.

Într-un sens mai larg, I^m este un ideal generat de monomii de gradul m . Aceste monomii sunt produse ale monomilor din I de la puterea m .

În schimb, I^m nu este un ideal generat de monomii de gradul m .

- (3.5) COROLAR. Dacă înmulțul R este unitar și $X \subset R$ este o mulțime, at.
(a) idealul (bilateral) $\langle X \rangle = \left\{ \sum_{i=1}^n r_i x_i s_i \mid r_i, s_i \in R, x_i \in X \text{ și } n \in \mathbb{N}^* \right\}$
(b) idealul stâng $\langle X \rangle = \left\{ \sum_{i=1}^n r_i x_i \mid r_i \in R, x_i \in X \text{ și } n \in \mathbb{N}^* \right\}$
(c) idealul drept $\langle X \rangle = \left\{ \sum_{i=1}^n x_i s_i \mid r_i \in R, x_i \in X \text{ și } n \in \mathbb{N}^* \right\}$.

(3.6) EXEMPLU (de ideal care nu e finit generat). Fie $V_R = C^{(\mathbb{N})} = \{f: \mathbb{N} \rightarrow \mathbb{C} \}$ împreună cu adunarea

$$(f+g)(n) := f(n) + g(n), \quad \forall n \in \mathbb{N}$$

și înmulțirea

$$(fg)(n) := f(n)g(n), \quad \forall n \in \mathbb{N}.$$

Fie $I \subset R$ dat prin $I = C^{(\mathbb{N})} = \{f: \mathbb{N} \rightarrow \mathbb{C} \mid f = 0 \text{ a.p.t.}\}$, unde $f = 0$ e.p.t. înseamnă că suportul $\text{Supp}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}$ este mulțime finită.

Cititorul poate probea că I este ideal în R . Deoarece I nu este finit generat (f, g)

atunci fie f_1, f_2, \dots, f_m o mulțime de generatori: $I = \langle f_1, f_2, \dots, f_m \rangle$. Fie

m un întreg mai mare decât toti întregii din $\text{Supp}(f_1) \cup \dots \cup \text{Supp}(f_m)$. Si considerăm $f \in I$ dat prin $f(m) = 1$ și $f(i) = 0$ pt. $i \neq m$. Deoarece $f \in \langle f_1, f_2, \dots, f_m \rangle$ rezultă că $f = g_1 f_1 + \dots + g_m f_m$, unde $g_1, \dots, g_m \in R$. În particular,

$f(m) = g_1(m)f_1(m) + \dots + g_m(m)f_m(m)$ înseamnă $1 = 0$, contradictie.

(3.6) PROP. Fie $f: R \rightarrow S$ un morfism de inele.

- (a) Dacă $\mathfrak{j} \subseteq S$ este un ideal (sau ideal stăng sau ideal drept), atunci un ecuații fel de ideal este $f^{-1}(\mathfrak{j})$. În particular, $f^{-1}(\langle 0 \rangle) = \text{Ker } f$ este ideal în R .
(b) Dacă f este surjectiv (i.e., epimorfism), atunci imaginea $f(I)$, a unui ideal (ideal stăng, ideal drept) $I \subset R$, este un ideal de ecuații fel în S .

Există o corespondență bijectivă cu părtenea inclusiunii între idealele (idealele stăng, idealele drept) din S și idealele de ecuații fel din R care conțin pe $\text{Ker } f$, dată de $\mathfrak{j} \subseteq S \longmapsto f^{-1}(\mathfrak{j}) \subseteq R$.

Dem. (a) Fie $\mathfrak{j} \subseteq S$ un ideal și fie $I := f^{-1}(\mathfrak{j})$. Arătăm că I este ideal în R .

Fie $x, y \in I$. Atunci, $\exists u, v \in \mathfrak{j}$ s.a.t. $u = f(x)$, $v = f(y)$. Rezultă $u - v = f(x - y)$, sau $x - y \in f^{-1}(\{u - v\}) \subseteq f^{-1}(\mathfrak{j})$. Acum, fie $r \in R$ și $s = f(r)$. Din $f(rx) = f(r) \cdot f(x)$, sau $\in \mathfrak{j}$ rezultă $rx \in f^{-1}(\mathfrak{j}) = I$. Analog, $xr \in I$, deci I este ideal.

(b) Punem $\mathfrak{j} := f(I)$. Dacă $u, v \in \mathfrak{j}$, at. fie $x, y \in I$ s.a.t. $u = f(x)$, $v = f(y)$.

Așa că $u-v = f(x) - f(y) = f(x-y) \in f(I)$, deci $x-y \in I$. Deoarece $x-y \in I$, atunci $su = f(x)f(x) = f(rx) \in f(I)$, pentru că $rx \in I$. Analog, $u \in f(I)$.

Notăm ϕ aplicația $J \subseteq S \mapsto f^{-1}(J)$. $\text{Ker } f \subseteq f^{-1}(J)$ deci
 $\langle 0 \rangle \subseteq J \Rightarrow f^{-1}(\langle 0 \rangle) \subseteq f^{-1}(J)$. Fie ψ aplicația $I \subseteq R \mapsto f(I) \subseteq S$.

Vom arăta că $I = f^{-1}(f(I))$: dacă $x \in I$, atunci $f(x) \in f(I) \Leftrightarrow x \in f^{-1}(f(I))$; invers, dacă $x \in f^{-1}(f(I))$, atunci $f(x) \in f(I)$, respectiv $f(x) = f(y)$, $y \in I$. Mai departe,
 $f(x-y) = 0 \Rightarrow x-y \in \text{Ker } f \subseteq I$. Dacă $x-y \in I \Leftrightarrow y \in I \Rightarrow x \in I$.

Vom arăta că $J = f(f^{-1}(J))$: fie $u \in J$ și fie $x \in R$ astfel încât $f(x) = u$. Atunci,
 $x \in f^{-1}(J)$ și aplicația f rezultă că $u = f(x) \in f(f^{-1}(J))$. Invers,
fie $u \in f(f^{-1}(J))$; atunci $u = f(x)$, unde $x \in f^{-1}(J)$. Rezultă că $u = f(x) \in J$.

În definitiv, am arătat că $(\phi \circ \psi)(I) = I \Leftrightarrow (\psi \circ \phi)(J) = J$, ceea ce înseamnă că aplicațiile ϕ și ψ sunt inverse (a se vedea și exerc. 3.11).

(3.7) TEOR. Fie R un inel și $I \subseteq R$ un ideal. Aplicația $\pi: R \rightarrow R/I$ datează prin $r \mapsto r+I$ este un morfism surjectiv de inele cu nucleu $\text{Ker } \pi = I$.

In plus, există o corespondență bijectivă între idealele lui R care contin pe I și idealele \bar{I} din R/I datează prin $\bar{I} \mapsto I = \pi^{-1}(\bar{I})$.

Dem. Exercițiu. \square (H.B. Bogla, fragment e pb. 25/p.34 din B.B.D.M.) Veroare: $\rightarrow \otimes$

Dacă $I, J \subseteq R$ sunt două ideale (ideale st., ideale dr.), atunci

a) $I+J = \{x+y \mid x \in I, y \in J\}$

este un ideal în R , numit suma idealelor I, J .

b) $I \cdot J = \langle xy \mid x \in I, y \in J \rangle = \left\{ \sum_{i=1}^m x_i y_i \mid x_i \in I, y_i \in J, m \geq 1 \right\}$

este un ideal în R , numit produsul idealelor I, J .

(3.8) TEOR. (prima teoz. de izomorfism). Dacă $f: R \rightarrow S$ este un morfism de inele, atunci f inducă un izomorfism de inele $R/\text{Ker } f \cong \text{Im } f$.

Dem. (Schilit) Aplicația $\bar{f}: R/\text{Ker } f \rightarrow \text{Im } f$ datează prin $\bar{f}: r + \text{Ker } f \mapsto f(r)$
este izomorfism de inele. \bar{f} este bine definită deoarece dacă $r' \equiv r \pmod{\text{Ker } f}$, atunci $r' - r \in \text{Ker } f \Rightarrow f(r') = f(r)$. \blacksquare

* Se se determine ideale din \mathbb{Z}_m si numarul lor, unde $m \in \mathbb{N}$, $m \geq 2$.

Sol. I o coresp. bij.

(3.9) TEOR (a doua teor. de izomorfism). Dacă $I \neq J$ sunt două ideale în anelul R , atunci

$$I/(I \cap J) \cong (I+J)/J.$$

Dem. Considerăm morfismul compunere $f: I \xrightarrow{\subseteq} I+J \xrightarrow{\pi} (I+J)/J$.
 $x \in I$ este în nucleul lui f dacă $f(x) = x+J = J$, deci $x \in J$. Astăzi,
 $\text{Ker } f = I \cap J$. Din prima teor. de izomorfism rezultă că $I/I \cap J \cong \text{Im } f$.

Dacă arătăm că $(I+J)/J \subseteq \text{Im } f$, atunci $(I+J)/J = \text{Ker } f$: $\hat{x} \in (I+J)/J \Rightarrow$
 $\hat{x} = (x+y) + J$, unde $x \in I$ și $y \in J \Rightarrow \hat{x} = x+J$, unde $x \in I$, deci $\hat{x} \in \text{Ker } f$. ■

(3.10) TEOR. (a treia teor. de izomorfism). Dacă $I \subset J$ sunt două ideale în anelul R , atunci J/I este un ideal în R/I și există un izo-
morfism de inele $(R/I)/(J/I) \cong R/J$.

Dem. Aplicăm $f: R/I \rightarrow R/J$ date prin $f(r+I) = r+J$ este un epimorfism.
 $\text{Ker } f = \{r+I \mid f(r+I) = J\} = \{r+I \mid r+I+J = J\} = \{r+I \mid r \in J\} = J/I$. Cu
prima teor. de izomorfism obținem $(R/I)/(J/I) \cong R/J$. ■

(3.11) EXERCITIU. Fie R, S două mulțimi și $f: R \rightarrow S$ o funcție.

(i) Pt. orice $A \subseteq R$ avem $A \subseteq f^{-1}(f(A))$.

(ii) Pt. orice $B \subseteq S$ avem $f(f^{-1}(B)) \subseteq B$ și $f(f^{-1}(B)) = B \cap f(R)$.

(iii) Dati exemplu în care incluziunile de la (i) și (ii) sunt stricte.

(iv) Fie $B_1, B_2 \subseteq S$. Dacă $B_1 \subseteq B_2$, at $f^{-1}(B_1) \subseteq f^{-1}(B_2)$; dar imaginea inversă nu este o funcție.

(v) $f(A) \subseteq B \Leftrightarrow A \subseteq f^{-1}(B)$.

Clase speciale de ideale

In aceasta lecție vom lucra, dacă nu se face altă precizare, în inele comutative unitare devințe idealele la care ne vom referi au un impact mare în aceste inele.

1. Ideale prime

In general, într-un inel R există divizori ai lui zero, adică elemente nenele $a, b \in R$ cu $ab = 0$. Ne interesează ce proprietăți să aibă un ideal $I \subseteq R$ pentru ca închil factor R/I să nu aibă divizori ai lui zero, altfel spus, R/I este inel integrum sau domeniu de integritate. Inelul R/I este integrum dacă oricare ar fi $\hat{a}, \hat{b} \in R/I$, $\hat{a} \cdot \hat{b} = \hat{0} \Rightarrow \hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$. În termeni echivalenți modulul I , cerința de inel integrum înseamnă

$$a \cdot b \in I \Rightarrow a \in I \text{ sau } b \in I.$$

Se ajunge la definiția următoare.

1.1. DEFIN. Fie R un inel comutativ unitar. Un ideal $P \subset R$ este ideal prim dacă $P \neq R$ și pentru orice două elemente $a, b \in R$,

$$ab \in P \Rightarrow a \in P \text{ sau } b \in P, \quad (1)$$

1.2. OBS. În cazul în care R nu e comutativ, dacă P este ideal prim, atunci are loc următoare proprietate: oricare ar fi I, J ideale în R ,

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ sau } J \subseteq P. \quad (2)$$

Invers, din (2) rezultă (1) dacă R este comutativ.

1.3. EXEMPLE. Idealul zero ($\text{adiu}, \langle 0 \rangle$) este prim în orice inel integrum devințe $ab = 0 \Rightarrow a = 0$ sau $b = 0$.

Dacă p este un întreg prim, atunci idealul principal $\langle p \rangle = p\mathbb{Z}$ este prim în \mathbb{Z} devințe

$$ab \in \langle p \rangle \Rightarrow p | ab \Rightarrow p | a \text{ sau } p | b \Rightarrow a \in \langle p \rangle \text{ sau } b \in \langle p \rangle.$$

1.4. PROP. Fie $\varphi: R \rightarrow S$ un morfism de inele.

(a) Dacă $J \subseteq S$ este ideal prim, atunci $\varphi^{-1}(J)$ este ideal prim în R ;

(b) Dacă φ este epimorfism și P este un ideal prim în R a.t. $P \supseteq \text{Kerf}$, atunci

$P' = \varphi(P)$ este ideal prim în S .

Dem. (a) Se zice că $\varphi^{-1}(J)$ este ideal în R și să dem. J este prim. Fie $a, b \in R$ s.t. $a \cdot b \in \varphi^{-1}(J)$. Atunci $\varphi(a \cdot b) \in J$, deci $\varphi(a) \cdot \varphi(b) \in J$. Pentru că J este prim, $\varphi(a) \in J$ sau $\varphi(b) \in J$, prin urmare $a \in \varphi^{-1}(J)$ sau $b \in \varphi^{-1}(J)$. Condiția $\varphi^{-1}(J) \neq R$ este înăglindată pentru că $1_S \notin J \Rightarrow \varphi^{-1}(1_S) \notin \varphi^{-1}(J)$.

(b). Se zice că $\varphi(P) \subseteq S$ este ideal. Să arătăm că $P' = \varphi(P)$ este prim: fie $a', b' \in S$ s.t. $a' \cdot b' \in P'$. Fie $a' = \varphi(a)$, $b' = \varphi(b)$, unde $a, b \in R$. Atunci $\varphi(a \cdot b) = a' \cdot b' \in P' = \varphi(P) \Rightarrow \exists p \in P$ s.t. $\varphi(a \cdot b) = \varphi(p)$, de unde $a \cdot b = p + e$ cu $p \in P$ și $e \in \text{Ker } \varphi$. Cum $\text{Ker } \varphi \subseteq P$ rezultă că $a \cdot b \in P$, de unde $a \in P$ sau $b \in P$. Atunci, $a' = \varphi(a) \in P'$ sau $b' = \varphi(b) \in P'$. Să arătăm că $P' + S : 1_R \notin P$. Deoarece $\varphi(1_R) \in \varphi(P)$, există $\exists p \in P$ s.t. $\varphi(1_R) = \varphi(p)$, deci $1_R - p \in \text{Ker } \varphi$. Rezultă că $1_R \in P$, contradicție. Prin urmare, $\varphi(1_R) \in S \setminus P'$. ■

(1.5) TEOR. Fie R un inel comutativ unitar cu $1 \neq 0$. Atunci un ideal $P \subset R$ este prim dacă și numai dacă R/P este inel integru.

Dem. Am văzut mai susa că \mathcal{I} de la R/P este inel integru, atunci P este ideal prim. Învers, fie P ideal prim și fie $\hat{a}, \hat{b} \in R/P$ s.t. $\hat{a} \cdot \hat{b} = \hat{1}$. Fie $a \in \hat{a}$ și $b \in \hat{b}$. Condiția $\hat{a} \cdot \hat{b} = \hat{1}$ înseamnă că $a \cdot b \equiv 0 \pmod{P}$, respectiv $a \cdot b \in P$. Rezultă că $a \in P$ sau $b \in P$, ori $a \equiv 0 \pmod{P}$, sau $b \equiv 0 \pmod{P}$, respectiv $\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$. ■

(1.6) cor. Idealele prime ale inelului \mathbb{Z}_n , $n > 1$ sunt de forma $\hat{p} \mathbb{Z}_n$, unde p este un nr. prim care divide pe n .

Dem Aplicând condiția $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ este surjectivă, iar idealele prime din \mathbb{Z} sunt generate de nr. prime. Conform Prop. 1.4, idealele prime din \mathbb{Z}_n sunt imaginiile $\hat{p} \mathbb{Z}_n$, p prim și $\langle p \rangle \supseteq \text{Ker } \pi = n\mathbb{Z} = \langle n \rangle$, adică $p \mid n$. (Altfel prob. 25/p.31 din B.B.D.M.)

9. Ideale maxime

Ce cond. tb. nu înăglindă idealul $I \subset R$ pentru a înelul factor R/I să fie wip? În primul rând, $\hat{1} \neq \hat{0}$ ca și cum sănătățea că $1 \notin I$, deci $I \neq R$. Apoi, dacă $\hat{a} \neq \hat{0}$, $\exists b \in R/I$ s.t. $\hat{a} \cdot \hat{b} = \hat{1}$. Deci, dacă $a \notin I$, atunci $ab - 1 \in I$,

de aici, $I \in I + \langle a \rangle$, respectiv $R = I + \langle a \rangle$. Ac. inseamnă că orice ideal care conține strict pe I va fi deasupra lui I .

(2.1) DEF. Fie R un inel comutativ unitar. Idealul $M \subset R$ s.n. maximal dacă $M \neq R$ și orice ideal $I \subset R$ cu $I \neq M$ și $M \subset I \subset R$ său $I = M$ sau $I = R$.

(2.2) EXEMPLU. Idealul $\langle 5 \rangle$ este maximal în \mathbb{Z} ; idealul $\langle 10 \rangle$ nu este maximal deoarece $\langle 10 \rangle \subset \langle 5 \rangle$

(2.3) PROPR. Fie R un inel comutativ unitar. Idealul $\langle 0 \rangle$ este maximal în R dacă și numai dacă R este corp.

DIM. Fie R un corp și fie $I \subset R$ un ideal $I \neq \langle 0 \rangle$. Dacă $a \in I$, $a \neq 0$, atunci $a \cdot a^{-1} \in I$, deci $1 \in I$. Invers, presupunem că $\langle 0 \rangle$ este maximal și fie $a \in R$, $a \neq 0$. Deoarece $\langle a \rangle = R$ rezultă că $1 \in \langle a \rangle$, deci $\exists b \in R$ s.t. $ab = 1$. ■

(2.4) TEOR. Fie iM un ideal în inelul comutativ unitar R . Urmt.

Afirm. sunt echivalente

- M este maximal
- R/M este corp.

DIM. (a) \Leftrightarrow (b). Fie $\hat{a} \neq 0$ în inelul factor R/M . Atunci $a \notin M$ și idealul $M + (a) = R$, deoarece $(a) + M \not\subset M$. Urmează că $m + ra = 1$, unde $m \in M$ și $r \in R$. Mai departe, $1 - ra = m \in M$ implica $\hat{1} = \hat{r}\hat{a}$, respectiv $1 = \hat{r} \cdot \hat{a}$.

(2.5) TEOR. Într-un inel comutativ unitar cu $1 \neq 0$ orice ideal este conținut într-un ideal maximal.

DIM. Folosim lema lui Zorn: Dacă A este o mulțime parțial ordonată în care orice parte total ordonată are un majorant în A , atunci A conține un element maximal.

Fie R un inel, $I \subset R$ un ideal și fie A mulțimea tuturor idealelor I' care conțin pe I . Fie $(I_j)_{j \in J}$ o mulțime de ideale total ordonată în incluziunea. Punem $I' := \bigcup_{j \in J} I_j$. Afirm că I' este ideal: subaditivitate

dacă $x, y \in I'$, atunci există $i, k \in \{1, \dots, n\}$. $x \in I_i$, $y \in I_k$. A total ordonare $\Rightarrow I_i \subseteq I_k$ sau $I_k \subseteq I_i$. Conspunțor, $x - y \in I_k$ sau $x - y \in I_i$. Prin urmare $x - y \in I'$. Dacă $r \in R$, atunci $rx \in I_i \subseteq I'$. În fine, $I' \neq \emptyset$ și urmărește că există un element maxim în I' . Dacă $a \in I' \Rightarrow \exists j \in \{1, \dots, n\}$ s.t. $a \in I_j$, deci $I_j = R$. Aplicând lema lui Zorn rezultă că în multimea A există un element maximal; în fapt, în multimea A există un ideal maximal ce conține pe I .

(2.6) COROLAR. În orice inel comutativ unitar nu există ideale maxime.

(2.7) TEOREMĂ (Lema chineză a resturilor). Fie I_1, I_2, \dots, I_n ideale în inelul R a.s. $R^2 + I_i = R$, $\forall i$ și $I_i + I_j = R$, $\forall i \neq j$. Dacă $b_1, b_2, \dots, b_n \in R$, atunci există $b \in R$ s.t.

$$b \equiv b_i \pmod{I_i}, \quad \forall i.$$

Meru multă b este unic determinat printr-o combinație congruentă modulide ideale
 $I_1 \cap I_2 \cap \dots \cap I_n$

Dem. Meru întâi să observăm că dacă R este inel unitar, atunci cond.
 $R^2 + I_i = R$ este autometră și următoarea părțe a teoremei.

Din $I_1 + I_2 = R$ și $I_1 + I_3 = R$ rezultă că

$$R^2 = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_1 I_2 + I_1 I_3 + I_2 I_3 \subseteq I_1 + I_2 I_3 \subset I_1 + I_2 \cap I_3.$$

Rezultă că

$$R = R^2 + I_1 \subset I_1 + (I_1 + I_2 \cap I_3) = I_1 + I_2 \cap I_3,$$

dacă $R = I_1 + I_2 \cap I_3$. Presupunem că $R = I_1 + (I_2 \cap I_3 \cap \dots \cap I_{k+1})$ și arătăm că $R = I_1 + (I_2 \cap I_3 \cap \dots \cap I_k)$. Într-adevăr,

$$R^2 = (I_1 + (I_2 \cap \dots \cap I_{k+1}))(I_1 + I_k) \subset I_1 + (I_1 \cap I_2 \cap \dots \cap I_k),$$

implică

$$R = I_1 + R^2 = I_1 + (I_1 \cap \dots \cap I_k).$$

Adăugăm, $R = I_1 + \bigcap_{i=1}^k I_i$ și în general $R = I_k + \bigcap_{i=k}^n I_i$. Acum, pt. fiecare $b_k \in R$, $\exists a_k \in I_k$ și $r_k \in \bigcap_{i \neq k} I_i$ s.t. $b_k = a_k + r_k$. Rezultă că

$$b_k \equiv r_k \pmod{I_k} \text{ și } r_k \equiv 0 \pmod{I_i}, \text{ pt } i \neq k.$$

Fie $b = r_1 + r_2 + \dots + r_n$. Atunci, $b \equiv b_i \pmod{I_i}$, $\forall i$. În fine, dacă $c \in R$ are proprietatea $c \equiv b_i \pmod{I_i}$, $\forall i$, atunci $c \equiv b \pmod{\bigcap_{i=1}^n I_i}$, prin urmare $c - b \in \bigcap_{i=1}^n I_i$, $\forall i$. Prin urmare $c - b \in \bigcap_{i=1}^n I_i$. ■

(2.8) COROLAR. (Lema chineză a resturilor). Fie $m_1, m_2, \dots, m_n \in \mathbb{Z}_+$ astfel că $(m_i, m_j) = 1$ pentru toți $i \neq j$. Dacă b_1, \dots, b_n sunt nr. întregi, atunci sistemul de congruențe

$$x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_n \pmod{m_n}$$

are o soluție unică determinată modulo $m_1 \dots m_n$.

Dem. Aici $I_i = (m_i)$ și $\bigcap_{i=1}^n I_i = (m_1 \dots m_n)$. Cond. $(m_i, m_j) = 1 \Rightarrow I_i + I_j = \mathbb{Z}$.
 Dacă se aplică Tez. 2.7. \blacksquare

1. a) Dati un exemplu de un morfism nornil de inele unitare $f: R \rightarrow S$ a.i. $f(1_R) \neq 1_S$.
- b) Dacă $f: R \rightarrow S$ este epi de inele unitare, at $f(1_R) = 1_S$.
- c) Dacă $f: R \rightarrow S$ este morfism de inele unitare și $u \in U(R)$ este a.s. $f(u) \in U(S)$, at. $f(1_R) = 1_S$ și $f(u^{-1}) = (f(u))^{-1}$ (dici $u \in U(R)$, at. nu rezultă $f(u) \in U(S)$).

Sol. a) Hesăză $e = f(1)$. Din $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow e = e^2$, deci e este idempotent în S . Așadar, $f: \mathbb{Z} \rightarrow \mathbb{Z}_6$, $1 \mapsto \bar{3}$, respectiv $m \mapsto \widehat{3m}$ îndeplinește cond. cerute.

b) $\exists r \in R$ a.s. $1_S = f(r)$. Atunci $f(r^m) = 1_S$, $\forall n \in \mathbb{N}$. $f(r^m + r^n) = f(r^m) + f(r^n)$, $m > n \Rightarrow f(r^m(1+r^{m-n})) = 1+1 \Rightarrow f(r^m) \cdot f(1+r^{m-n}) = 1+1 \Rightarrow 1(f(1)+1) = 1+1$, $f(1) = 1$.

c) $f(u \cdot 1) = f(u) \Rightarrow f(u) \cdot f(1_R) = f(u) \Rightarrow f(u)[f(1_R) - 1_S] = 0$. $\forall u \in f(u)$ este inversabil $\Rightarrow [f(u)]^{-1} \cdot f(u)[f(1_R) - 1_S] = 0 \Rightarrow f(1_R) = 1_S$.

Din $u \cdot u^{-1} = 1_R$ și $f(u) \cdot f(u^{-1}) = 1_S$ și $f(u) \cdot [f(u)]^{-1} = 1_S \Rightarrow f(u^{-1}) = [f(u)]^{-1}$, folosind proprietatea de unicitate a inversului.

2. Un element $a \in R$, R inel, este nilpotent dacă $\exists n > 1$ a.i. $a^n = 0$.

Dacă R comutativ și a, b nilpotente, atunci $a+b$ este nilpotent.

3. Într-un inel R a.e. :

- a) R nu are elemente nilpotente nemile;
- b) dacă $a \in R$ și $a^2 = 0$, at. $a = 0$.

Sol. a) \Rightarrow b) este evident. b) \Rightarrow a). Presupunem $b^m = 0$. Dacă m este par, at $b^m = b^{\frac{m}{2}} \cdot b^{\frac{m}{2}}$ $\Rightarrow b^{\frac{m}{2}} = 0$; dacă m este impar, at $b^{m+1} = 0 \Rightarrow b^{\frac{m+1}{2}} = 0$. Dacă m nu este jumătate de par, așezăm la $b^2 = 0$, obținându-se următorul ciclu:

$n; \frac{n}{2}; \text{ sau } \frac{n+1}{2}; \frac{n}{4}; \text{ sau } (\frac{n}{2}+1)/2; \text{ sau } \frac{n+1}{4}; \text{ sau } \frac{n+1}{2}+1; \dots$
este strict descrescător.

4. Mult. elem. nilpotente dintr-un inel comutativ form. un ideal.

5. Fie I ideal într-un inel comutativ R și fie $\text{Rad } I := \{n \in \mathbb{N} \mid n^m \in I\}$, pentru un $m > 0$. Arătați că $\text{Rad } I$ este un ideal.

6. Fie $I \subseteq R$ un ideal în inelul R și $\text{fie } [R:I] = \{x \in R \mid x \cdot I \subseteq I, \forall x \in R\}$. Arătați

$\mathcal{I}[R:I]$ este un ideal care conține I .

7. Fie R un inel unitar și $M_m(R)$ inelul matricelor patrate de ordinul m cu elemente din R . Aruncă

$J \subseteq M_m(R)$ este ideal $\Leftrightarrow J = M_m(I)$, unde I este ideal în R .

Ind. Fie J și $I = \{a_{ij} \mid A = (a_{ij}) \in J\}$. Dacă $E_{rs} = (S_{ij}^{rs})$, unde $S_{ij}^{rs} = 1$, dacă $(i,j) = (r,s)$ și $S_{ij}^{rs} = 0$ în rest, atunci pt. o matrice $A = (a_{ij})$, $E_{p,r}AE_{s,q}$ este matricea cu 1-urile în poziția (p,q) și 0 în rest. Rezultă că pt orice $A \in J$, elem $a_{rs} \in I$ deci $E_{1,r}AE_{s,1} \in J$ și are în poziția $(1,1)$ pe 1-ură. ■

2. Dacă H este idealul elem. nilpotente într-un inel comutativ R , atunci R/H este un inel fără elemente nemulte nilpotente.

3. (a) Un inel unitar R este un corp $\Leftrightarrow R$ nu are ideale proprii.

(b) Dacă R este un inel (nu neapărat unitar) fără ideale de st. proprii, atunci suntem $R^2 = 0$ sau R este un corp.

Ind. Aratăți că $\{a \in R \mid Ra = 0\}$ este un ideal. Dacă $cd \neq 0$, arătați că $\{r \in R \mid rd = 0\} = 0$. Dacă $e \in R$ are propriet. $ed = d$, atunci e este unitate.

Descompunerea în factori în inele comutative (I)

Inelul întregilor \mathbb{Z} este exemplul standard de inel în care orice element nenul are o descompunere unică în factori primi. Totuși, generalizarea noțiunilor familiare, precum divizibilitate, prim, ireductibil etc. va evidenția semnificație nouă care, pe de alturi, depășește lumenul său comun. Cu toate acestea, proprietăți fundamentale și algoritmi sunt analogi inelului întregilor.

1. DEF. Fie R un inel comutativ. Se spune că elementul nenul $a \in R$ divide elementul b și se scrie $a|b$ dacă $\exists x \in R$ astfel încât $ax = b$.

Elementele $a, b \in R$ sunt associate în divizibilitate (sau, mai simplu, asociate) dacă $a|b$ și $b|a$; în acest caz scriem $a \sim b$.

De exemplu, în \mathbb{Z}_{12} avem $2|10$, dar și $10|2$, deci $2 \sim 10 \cdot 5$. Tot astfel, în $\mathbb{R}[x]$ polinoamile $3x^2 + 3$ și $5x^2 + 5$ sunt asociate.

Holințea de divizibilitate poate fi exprimată în termeni de ideale principale, astăzi cum rezultă din propoziția următoare.

2. PROP. Fie $a, b \in R$, unde R este un inel comutativ unitar.

- (i) $a|b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$;
- (ii) $a \sim b \Leftrightarrow \langle a \rangle = \langle b \rangle$;
- (iii) $u \in R$ este o unitate $\Leftrightarrow u|r$ pentru toti $r \in R$;
- (iv) $u \in R$ este o unitate $\Leftrightarrow \langle u \rangle = R$;
- (v) Relația de asociere \sim este o relație echivalență pe R ;
- (vi) Dacă $a = bu$, unde $u \in U(R)$, atunci $a \sim b$. Dacă R este inel întreg, atunci reciprocă este adevărată.

Dem. Exercițiu. ■

3. DEF. Fie R un inel comutativ unitar. Un element $c \in R$ s.n. ireductibil dacă

- (i) c este nenul și neînversabil;
- (ii) $c = ab \Rightarrow a$ sau b este o unitate, de unde, $c \sim a$ sau $c \sim b$.

Dacă elementul $p \in R$ să nu fie prim de către

- (i) p este nuanță și nu este inversabil;
- (ii) $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$.

4. EXEMPLU. Dacă $p \in \mathbb{Z}$ este un nr. prim, atunci p și $-p$ sunt despuțiv elemente ireductibile și prime.

In anelul \mathbb{Z}_6 , elementul 2 este prim deoarece $2 \mid ab \Rightarrow ab = 2c$, prin urmare, ab este multiplu de 2. Așadar $a = 2a'$ și $b = 2b'$. Totuși, 2 nu este ireductibil pentru că $2 = 2 \cdot 1$ și nici 2 nici 4 nu este inversabil.

Pe de altă parte, există elemente ireductibile care nu sunt prime. De ex.,

în anelul $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$, 2 este ireductibil deoarece daca

$$2 = (a + b\sqrt{10})(c + d\sqrt{10}) \Rightarrow ac + 10bd = 2 \text{ și } ad + bc = 0.$$

$$\text{Deci } acd + 10bd^2 = 2d \text{ și } acd + bc^2 = 0 \Rightarrow b(c^2 - 10d^2) = 2d \text{ și inced}$$

$$b(c - d\sqrt{10})(c + d\sqrt{10}) = (a + b\sqrt{10})(c + d\sqrt{10}).d.$$

După simplificare se obține $b(c - d\sqrt{10}) = (a + b\sqrt{10})d$, respectiv $bc - bd\sqrt{10} = ad + bd\sqrt{10}$. Trebuie ca $-bd = +bd$,

respectiv $bd = 0$. Dacă $d = 0$, atunci $2 = (a + b\sqrt{10})c \Rightarrow b = 0$ și $ac = 2$. Prin urmare, $|a| = 1$ sau $|c| = 1$, adică unul din factorii descompuneri

$2 = (a + b\sqrt{10})(c + d\sqrt{10})$ este o unitate. Pe de altă parte, 2 nu este prim deoarece $2 \mid (4 + \sqrt{10})(4 - \sqrt{10})$, dar 2 nu divide niciunul

dintre factorii produsului.

Există o legătură strânsă între elem. prime și idealele prime, resp. între elementele ireductibile și idealele maximale.

5. PROP. Fie p și c două elemente nuanță într-un anel integral.

- (i) p este prim $\Leftrightarrow \langle p \rangle$ este ideal prim;
- (ii) c este ireductibil $\Leftrightarrow \langle c \rangle$ este un elem. maximal în mulțimea S a tuturor idealelor principale din R ;
- (iii) Orice prim este ireductibil;
- (iv) Dacă R este, în plus, anel principal, atunci ireductibil este prim.
- (v) Orice asociat al unui ireductibil (resp. prim) este, de asemenea, ireductibil (resp. prim)
- (vi) Singurii divizori ai unui elem. ireduct. sunt elem. asociate și unireabile din R .

Dem (i) exercitiu.

(ii). Fie c ired. At. $c \notin U(R)$, deci $(c) \neq R$. Acum, $\forall c \in (c) \subseteq (d)$. Avem $c = dx$. Cum c ired $\Rightarrow d$ sau x este inversabil, deci $(d) \subseteq R$ sau $(d) = (c)$. Astăzi, $\langle c \rangle$ este maximal în S . Invers, pres. că $\langle c \rangle$ este maximal în S . At., c nu este inversabil, deci $\langle c \rangle \neq R$. Acum, dacă $c = ab$, atunci $\langle c \rangle \subseteq \langle a \rangle$, deci $\langle a \rangle = \langle c \rangle$ sau $\langle a \rangle = R$. În primul caz, $a = cy$, prin urmare $c = ab = cyb$. R fiind inel integral $\Rightarrow y = b$, deci $b \in U(R)$. În cazul, $\langle a \rangle = R$, și $a \in U(R)$. Deci, $c = ab \Rightarrow a \in U(R)$ sau $b \in U(R)$, fapt care înseamnă că c este ireductibil.

(iii) Fie $p \in R$ element prim. Dacă $p = ab$, și $p \mid a$ sau $p \mid b$. Să pres. că $p \mid a$. Atunci, $a = px$ și $p = ab = pxb$; după simplificare, $1 = bx$ și deci, b inversabil. În concluzie, c este ireducibil.

(iv) Fie p ired. în inelul principal R . Atunci $\langle p \rangle$ este maximal în S . $\langle p \rangle$ maximal $\Rightarrow \langle p \rangle$ prim, deci p prim.

(v) Pres. că c este ireducibil, și $d \mid c$. Punem $d = ab$. Pres. că $c = du$, u inversabil. At. $c = abu$, de unde a sau b nu inversabile. Dacă b nu inversabil, și b inversabil, deci d ireducibil. Dacă a inversabil, și d ireducibil. În ambele sit., b ireducibil.

(vi) Fie c ireducibil. $\exists a \mid c$. At. $(c) \subseteq (a)$, deci $(c) = (a)$ sau $(a) = R$. Dacă cele două situații $\Rightarrow a \mid c$ sau a inversabil.

Inelul \mathbb{Z} cu descompunerea întregilor în factori primi este exemplul standard de inel ce s-a deținut. Viz. din definiția următoare.

sau inel factorial

6. DEF. Un inel integral R este un domeniu cu descomp. unică.

(i) orice element nenul neinversabil $a \in R$ se poate scrie $a = c_1 c_2 \dots c_n$, cu c_i ireductibili;

(ii). dacă $a = c_1 c_2 \dots c_n$ și $a = d_1 d_2 \dots d_m$ (cu c_i, d_i ireductibili), atunci $n = m$ și există o permutare a mult. $\{1, 2, \dots, n\}$ astfel că $c_i \sim d_{\sigma(i)}$ pt. orice i .

7. OBS. Fie c ireducibil. $\exists a \mid ab$. At. $ax = ab \Rightarrow$ descomp. în factori primi a lui ab conține ireducibil c . Dacă c apărține factorilor lui a , și $c \mid a$, altfel $c \mid b$. Astăzi, în dom. cu descompunere unică, prim \Leftrightarrow ireductibil.

s-a definit inel principal?

8. LEMĂ. Dacă R este un inel principal \Leftrightarrow

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots \dots$$

este un lant ascendent de ideale în R , atunci există $n > 0$ s.t. $(a_n) = (a_j)$, $\forall j \geq n$ (se spune că lantul stăționar nu este stăționar).

Dem. Fie $I = \bigcup_{i \geq 1} \langle a_i \rangle$. Arătăm că I este ideal. Pt cărui, fie $x, y \in I$. Atunci $\exists i, j \in \mathbb{N}, x \in \langle a_i \rangle \wedge \exists k \in \mathbb{N}, y \in \langle a_k \rangle$. Dar $\forall j \leq k$, at. $x, y \in \langle a_k \rangle$, deci $x - y \in \langle a_k \rangle \subseteq I$.

Analog, dacă $x \in I \wedge \forall n \in \mathbb{N}$, at. $nx \in I$. Deoarece R este inel principal, $\exists a \in R$ a.s. $I = \langle a \rangle$, $a \in I$. Rezultă că $\exists m > 0$ s.t. $a \in \langle a_m \rangle$, deci $\langle a \rangle \subseteq \langle a_m \rangle$. Dacă $j \geq m$, atunci avem singură inclusiune

$$\langle a \rangle \subseteq \langle a_m \rangle \subseteq \langle a_j \rangle \subseteq I = \langle a \rangle,$$

de unde se obține $\langle a_m \rangle = \langle a_j \rangle$. \blacksquare

9. EXERCITII.

9.1. Un ideal nemulțim într-un inel principal este maximal d.s.m.d este prim.
În particular, $I = pR = \langle p \rangle$, p prim.

Sol. Se scrie că orice ideal maximul este prim. Învers, fie P ideal prim. At. $P = (p)$, p element prim. Cf. Prop. 5(iii), p este ireductibil. Înțeles că (p) este maximul (vezi Prop. 5(iv)).

9.2. Fie $R = \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$.

(a) Afili. $H: R \rightarrow \mathbb{Z}$ dată prin $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ este a.z.

$H(uv) = H(u) \cdot H(v)$ pt. t.c. $u, v \in R$ și $H(u) = 0 \Leftrightarrow u = 0$,

(b) u inversabil în $R \Leftrightarrow H(u) = \pm 1$:

(c) $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ sunt elemente ireductibile în R .

(d) $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ nu sunt prime în R .

9.3. Să se arate că în inelul $\mathbb{Q}[x, y]$ elementul $x^2 + y^2$ este ireductibil.

9.4(a) În inelul $\mathbb{Z}[\sqrt{-6}]$ are loc egalitatea $2 \cdot 3 = (\sqrt{-6})(-\sqrt{-6})$. Este $\mathbb{Z}[\sqrt{-6}]$ inel factorial?

(b) Inelele $\mathbb{Z}[\sqrt{-5}]$ și $\mathbb{Z}[\sqrt{26}]$ nu sunt factoriale.

Descompunerea în inele comutative (II)

10. TEOR. Orice inel principal este inel factorial. Adică, într-un inel în care orice ideal poate fi generat de un singur element, toate elementele nenule neinversabile au o descompunere unică (în sensul Def. 6).

Dem. Fie R un inel principal. Pres., prin absurd, că există $a \in R$, un element nenul neinversabil care nu se poate scrie ca un produs (finit) de elemente ireductibile. a nu poate fi ireductibil, deci ex. o descomp. a lui a de forma $a = a_1 a_1'$, în care nici a_1 , și nici a_1' nu sunt inversabile (a_1, a_1' sunt și nenule). De mult, cel puțin unul dintre elem. a_1, a_1' nu se descomp. în produs de elem. ireductibile, adică are proprietățile lui a .

Pres. că a_1 are proprietățile lui a . Atunci, un răsonament analog ar urmări sănătatea lui a_1 , conduce la un element a_2 care are proprietățile lui a_1 . Se obține un sănătate infinț de elem. nenule neinversabile din R , ceea ce contrazice teorema 8.

$$a = a_0, a_1, a_2, \dots,$$

cu proprietățea $a_i | a_j$ dacă și $i < j$. Acest sănătate infinț strict ascendent de ideale.

$$\langle a_0 \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots \quad (1)$$

Sănătate (1) contrazice teorema 8 care ne asigură că un astfel de sănătate nu poate exista.

Pentru unicitate, fie $c_1, c_2, \dots, c_m = a = d_1, d_2, \dots, d_m$ (c_i, d_j ireductibile).

$c_i | d_j \forall i, j$ și c_i prim (Prop. 5, (iv)) $\Rightarrow \exists j_i$ s.t. $c_i | d_{j_i}$. Dar singurii divizori ai unui elem. ireductibil sunt elem. asociate sau inversibile (cf. Prop. 5 (v)). În cazul nostru, $c_i \sim d_{j_i}$. Dacă $n \neq m$, $c_n \sim d_{j_n}$, de unde $m \leq n$. Un proces similar pentru $d_1, d_2, \dots, d_m \Rightarrow m \leq n$, deci $m = n$.

$\forall (j_1, j_2, \dots, j_n)$ este o permutare a mulțimii $\{1, 2, \dots, n\}$. ■

Inele principale și factoriale nu sunt singurile care au proprietăți deosebite printre inelele integre. Un alt fel de inel întreg este studiat în continuare.

11. DEF. Un inel comutativ R este inel euclidian dacă există o funcție

$\varphi: R \setminus \{0\} \rightarrow \mathbb{N}$ a. z. :

(i) dacă $a, b \in R$ și $ab \neq 0$, at. $\varphi(a) \leq \varphi(ab)$;

(ii) dacă $a, b \in R$ și $b \neq 0$, atunci există $q, r \in R$ a. z. $a = bq + r$, cu $r = 0$ sau $r \neq 0$ și $\varphi(r) < \varphi(b)$.

Un inel euclidian care nu este inel întreg este domeniu euclidian.

12. EXEMPLU. Inelul \mathbb{Z} al întregilor este domeniu euclidian cu $\varphi(x) = |x|$.

13. EXEMPLU. Un corp K este domeniu euclidian cu $\varphi(x) = 1$, $x \neq 0$.

14. APlicație. (a) Dacă a și n sunt întregi, $n > 0$, at. există întregii q și r a. z. $a = qn+r$, unde $|r| \leq n/2$.

Intr-o lămurire, $a = q'n + r'$, unde $0 \leq r' < n$. Dacă $r' \leq \frac{n}{2}$, atunci $q = q'$ și $r = r'$.

Dacă $r' > \frac{n}{2}$, atunci $\frac{n}{2} < r' < n \Rightarrow -\frac{n}{2} < r' - n < 0 \Rightarrow |r' - n| < \frac{n}{2}$ și

$a = (q'+1)n + (r' - n)$. Putem $q := q' + 1$ și $r = r' - n$.

(b) $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$, numit inelul întregilor lui Gauss, este domeniu euclidian. Cu $\varphi(a+bi) = a^2 + b^2$.

Coral (i) de DEF. 11 este evident și se face. Pentru (ii), fie $A = a+bi$ și $x \in \mathbb{Z}_{>0}$. Folosind (a),

$a = q_1 x + r_1$, și $b = q_2 x + r_2$, cu $|r_1| \leq x/2$ și $|r_2| \leq x/2$.

Atunci, $A = q_1 x + r$, unde $q = q_1 + q_2 i$, $r = r_1 + r_2 i$ și dacă $r \neq 0$, atunci

$$\varphi(r) = r_1^2 + r_2^2 \leq \frac{x^2}{4} + \frac{x^2}{4} < x^2 = \varphi(x).$$

Acum, fie $B = c+di \neq 0$. Avem $B\bar{B} = c^2 + d^2 > 0$. $\exists q, r_0 \in \mathbb{Z}[i]$ a. z.

$A\bar{B} = q B\bar{B} + r_0$, unde $r_0 = 0$ sau $r_0 \neq 0$ și $\varphi(r_0) < \varphi(B\bar{B})$. Avem

$\bar{B}(A-qB) = r_0$ și, ca notăție $r := A - qB$ rezultă $A = qB + r$, unde $r = 0$ sau $r \neq 0$. Dacă $r \neq 0$, at $\varphi(\bar{B} \cdot r) = \varphi(r_0) < \varphi(B\bar{B}) \Rightarrow \varphi(\bar{B}) \cdot \varphi(r) < \varphi(B) \cdot \varphi(r)$

$$\Rightarrow \varphi(r) < \varphi(B).$$

15.TEOR. Orice inel euclidian este inel principal unitar.

Denum. Fie $I \neq 0$ un ideal în R . Fie $a \in I$ propriet. $\varphi(a) = \min \{ \varphi(x) \mid x \neq 0, x \in I \}$. Acum, fie $b \in I$, $b = qa + r$ cu $r = 0$ sau $r \neq 0$ și $\varphi(r) < \varphi(a)$. Dar $r = b - qa \in I$ $\Rightarrow r = 0$, respectiv $b = qa$. Urmează că $I \subseteq Ra \subseteq I$, deci $I = Ra = \langle a \rangle$, astfel că R este principal.

Să arătăm că R este unitar. Pentru aceasta, folosim că R în sensul este un ideal, deci $R = \langle a \rangle$, $a \in R$. Atunci $a = ae = ea$, unde $e \in R$.

Fie $b \in R$. Atunci $b = xa$, pentru $x \in R$. Atunci

$be = (xa)e = x(ae) = xea = b$, deci e este un element unitate. \square

16. consecuță a Teor.10 și Teor.15, avem proprietatea următoare.

16.COR. Orice inel euclidian este factorial.

17.DEF. Fie $X \subset R$ o submultime în inelul comutativ R . Un element $d \in R$ este un cel mai mare divizor comun al lui X dacă:

- (i) $d | a$ pentru toți $a \in X$; c.m.m.d.c.
- (ii) $c | a$ pentru toți $a \in X \Rightarrow c | d$.

Hu întotdeauna există c.m.m.d.c. De exemplu, în inelul \mathbb{Z} întregul 2 nu are divizori, astfel că 2 și 4 nu au un c.m.m.d.c. Dacă R are unitate și a_1, a_2, \dots, a_n au pe 1 ca c.m.m.d.c., atunci a_1, a_2, \dots, a_n sunt relativ prime.

18.TEOR. Fie a_1, a_2, \dots, a_n elemente în inelul comutativ unitar R .

- (i) $d \in R$ este un cel mai mare divizor comun al mulțimii $\{a_1, a_2, \dots, a_n\}$ a.s. $d = r_1 a_1 + \dots + r_n a_n$, unde $r_i \in R$ $d = \text{l.c.m.} \{a_1, \dots, a_n\} = \langle a_1, \dots, a_n \rangle$;
- (ii) Dacă R este principal, atunci mult. $\{a_1, \dots, a_n\}$ are un cel mai mare divizor comun și oricare este de forma $r_1 a_1 + \dots + r_n a_n$ ($r_i \in R$);
- (iii) Dacă R este factorial, atunci oricare elemente a_1, a_2, \dots, a_n au un cel mai mare divizor comun.

Denum.(i), $\Rightarrow "d | a_i \Rightarrow \langle a_i \rangle \subseteq \langle d \rangle, \forall i \Rightarrow \langle a_1 \rangle + \dots + \langle a_n \rangle \subseteq \langle d \rangle$ Cum $d = \sum r_i a_i \Rightarrow$

$\langle d \rangle \subseteq \sum \langle a_i \rangle$.

\Leftarrow Este clar că $d = \sum d_i a_i$. Apoi, $\langle a_i \rangle \subseteq \langle d \rangle \Rightarrow d | a_i$, și. În fine, dacă $c | a_i$, și $\Rightarrow c | \sum d_i a_i$, deci $c | d$.

(ii) Folosind că $\exists d \in R$ astfel încât $\langle a_1 \rangle + \dots + \langle a_n \rangle = \langle d \rangle$,

(iii) Oricare $a_i = c_i^{m_{i1}} c_2^{m_{i2}} \dots c_s^{m_{is}}$, unde c_j ireductibile și $m_{ij} \geq 0$. Atunci $d = c_1^{k_1} \dots c_s^{k_s}$, unde $k_j = \min\{m_{1j}, m_{2j}, \dots, m_{sj}\}$. \blacksquare

19. EXERCITII

(1) Polinomul $X^2 + Y^2$ este ireductibil în inelul $\mathbb{Q}[X, Y]$, dar redusibil în $\mathbb{C}[X, Y]$.

(2) În inelul $\mathbb{Z}[i\sqrt{5}]$ elem. $2(1+i\sqrt{5})$ și 6 sunt c.m.m.d.c.

Sol. Mai întâi să se arate că $a+b\sqrt{5} | c+d\sqrt{5}$, atunci $\overline{a+b\sqrt{5}} | \overline{c+d\sqrt{5}}$, sau urmărește că $a^2+5b^2 | c^2+5d^2$. Notăm $H(a+b\sqrt{5}) := a^2+5b^2$. Procesul de calcul nu mai are divizori comuni. Deoarece 2 este un divizor comun, trebuie ca $2 | d$. De asemenea, $1+i\sqrt{5}$ este un divizor comun deoarece $6 = (1+i\sqrt{5})(1-i\sqrt{5})$.

Din $2 | d$ și $1+i\sqrt{5} | d \Rightarrow 4 | H(d)$ și $6 | H(d)$. Se obține că $12 | H(d)$.

Pe de altă parte, $d | 2(1+i\sqrt{5})$ și $d | 6 \Rightarrow H(d) | 24$ și $H(d) | 36$. Deoarece $36 = 12 \cdot 3$, rezultă că $H(d) | 12$. În definitiv, $H(d) = 12$, imposibil în $\mathbb{Z}[i\sqrt{5}]$.

(3) În inelul $\mathbb{Z}[i\sqrt{5}]$ elem. 3 și $1+i\sqrt{5}$ sunt c.m.m.d.c.

Sol. Procedând ca la exerc.(2) se găsește că 1 este un c.m.m.d.c.

(4) Folosind egalitatea $2 \cdot 3 = i\sqrt{6}(-i\sqrt{6})$ să se arate că inelul $\mathbb{Z}[i\sqrt{6}]$ nu este factorial.

(5) Inelele $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[\sqrt{26}]$, $\mathbb{Z}[i\sqrt{3}]$ nu sunt factoriale.

(6) Fie $R = \{f \in \mathbb{Z}[x] \mid f = a_0 + a_1 x + \dots + a_n x^n, n \neq 1\}$. Să se arate că

(i) $R = \mathbb{Z}[x^2, x^3]$;

(ii) c.m.m.d.c. $(x^2, x^3) = 1$ și c.m.m.m.c. (x^2, x^3) nu există;

(iii) c.m.m.d.c. (x^5, x^6) și c.m.m.m.c. (x^5, x^6) nu există;

(iv) x^2 este ireductibil, deci nu este prim. (B.B.D.H., p. 57)

L+116
Complemente de teoria inclelor

Ideale. Inclu factor

1. Relație de echivalență. O relație de echivalență este corespondența în matematică a unui criteriu de clasificare a elementelor unei multimi din lumea naturală, cum ar fi, de exemplu, clasificarea frunzelor după forma lor (sunt 13 clase de frunze). În lumea naturală criteriul de clasificare nu este foarte strict; de exemplu, o pupe poate avea caracteristiciile a două clase apropiate, dar acestea ambiguitate nu afectează clasificarea ca atare. În schimb, în matematică, relația de echivalență este un criteriu în apărute rigid: fără dubii, un element al multimii clasificate aparține unei singure clase. Precizare în clasificarea pe care să realizezeză rel. de echiv. între structuri algebrice permite transferul unei operațiuni de operării cu elementele multimii în operații cu clasele de echivalență. În cazul rel. de echivalență, criteriul de clasificare este mai mult sau mai puțin evident, semnificația sa necesitând un proces de reflexie.

(1) EXEMPLU. Fie D mult. dreptelor din spațiu real euclidian. Pe D definim rel. de echivalență: dacă $d, d' \in D$, atunci

$$d \equiv d' \text{ dacă } d = d' \text{ sau } d \cap d = \emptyset.$$

O clasă de echivalență este multimea tuturor dreptelor din spațiu paralele între ele și punctul numele de directe în spațiu.

(2) EXEMPLU. Impartirea nr. întregi în pere si impare se realizează definiind rel. de echivalență următoare: dacă $m, n \in \mathbb{Z}$, atunci

$$m \equiv n \text{ dacă } m - n \in 2\mathbb{Z}.$$

(3) EXEMPLU. După cum vom vedea, exemplul 2 este un caz particular al criteriului restul împărțirii la întregul pozitiv n , $n \geq 2$. Astfel, dacă $x, y \in \mathbb{Z}$, atunci

$$x \equiv y \pmod{n} \text{ dacă } x - y \in n\mathbb{Z}. \quad (1)$$

Se arată imediat că $x \equiv y \pmod{n}$ dacă și numai dacă x și y au același rest r , $0 \leq r \leq n-1$, la împărțirea cu n . Deoarece valoriile posibile ale lui r sunt $0, 1, 2, \dots, n-1$ rezultă că sunt n clase de echivalență, numite submultimiile $r + n\mathbb{Z}$, $r \in \{0, 1, \dots, n-1\}$. O notare ușoară este $\hat{r} := r + n\mathbb{Z}$.

(Dacă $n = 2$, atunci obținem exemplul 2.)

L7-2/6

Modalitatea în care se tratează, în continuare, împărțirea în clase moduale nu deține de rel. (1) este un model pentru oricare alt nivel. Cls. de echivalență, numite \hat{m} clase de resturi modulo m alcătuiesc o particiție a lui \mathbb{Z} , adică $\mathbb{Z} = \hat{0} \cup \hat{1} \cup \dots \cup \hat{m-1}$, reuniune disjunctă. Cu ajutorul oper. de adunare și înmulțire din inelul $(\mathbb{Z}, +, \cdot)$ se definesc oper. între clasele de resturi:

$$\hat{a} + \hat{b} \stackrel{\text{def}}{=} \hat{a+b} \quad \text{și} \quad \hat{a} \cdot \hat{b} \stackrel{\text{def}}{=} \hat{ab}. \quad (2)$$

Multimea $\mathbb{Z}/m\mathbb{Z} = \{\hat{0}, \hat{1}, \dots, \hat{m-1}\}$ împreună cu operațiile definite de (2) mențină structura de inel a lui \mathbb{Z} , în sensul că $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ este un inel. Inelul $\mathbb{Z}/m\mathbb{Z}$ se mai notează și \mathbb{Z}_m .

2. Ideale în inele comutative unitare. Deoarece ne fac să fie mai precise, peste tot R este un inel comutativ unitar cu $1 \neq 0$.

Intr-un inel se pot întâlni multe situații, neobișnuite și puțin evidențiate până în acest moment. De exemplu, pot exista elemente nemulți și cu același produs este zero: $\hat{2} \cdot \hat{3} = \hat{0}$ în \mathbb{Z}_6 sau $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ în $M_2(\mathbb{R})$. O altă situație este că inelul poate conține elemente care au puternice mulțimi începând cu un anumit ordin: în \mathbb{Z}_6 , avem $\hat{2}^n = \hat{0}$ pt. $n \geq 6$, $\hat{4}^n = \hat{0}$, pentru $n \geq 3$ ori în $M_3(\mathbb{R})$ avem $\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \end{pmatrix}^n = \hat{0}$ pt. $n \geq 3$. În fine, ca un ultim exemplu, intr-un inel pot exista elemente x care nu sunt inversibile și, de ex., $\hat{4}$ nu e inversabil în \mathbb{Z}_6 și $\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$ nu e inversabil în $M_2(\mathbb{R})$.

Pentru toate aceste situații „inconfortabile” o rezolvare pertinente este împărțirea elementelor inelului în clase de echivalență astfel încât situațiile evocate mai sus să fie luate sub control. Cheia rezolvării este noțiunea de ideal ($I \subseteq R$ este ideal dacă este parte stabilită în raport cu adunarea și înmulțirea din R și, în plus, $rx \in I$ pt. orice $r \in R$ și orice $x \in I$)

2.1. Hilberdicalul. Un element $x \in R$ este nilpotent dacă există un întreg $n > 0$ s.t. $x^n = 0$.

Nă

(4) PROP. Multimea tuturor elementelor nilpotente într-un inel R este un ideal și inelul factor R/I nu are elemente nilpotente.

Dem. Deoarece $x \in I$ și $x^n = 0$, atunci $(rx)^n = r^n x^n = 0$, deci $rx \in I$. Acum, dacă $x, y \in I$ și $x^m = 0$ și $y^n = 0$. Atunci $(x+y)^{m+n-1} = (x+y) \dots (x+y) = \sum x^r y^s$ și $r+s = m+n-1$. Deoarece $r \geq m$, atunci $x^r y^s = 0$. Deoarece $s \geq n$, atunci $x^r y^s = 0$. Astfel, toate produsele $x^r y^s$ sunt

egale cu zero și $\deg(x+y)^{m+n-1} = 0$, respectiv $x+y \in N$. În consecință, N este un ideal. Se arată că inelul factor R/N nu conține elemente nulpotente. Fie $\hat{x} \in R/N$ o clasa de echivalență și $x \in \hat{x}$ un reprezentant al ei. Atunci $\hat{x}^m \in R$ este un reprezentant al clasei $(\hat{x})^m$. Dacă $(\hat{x})^m = \hat{0}$, atunci $x^m \in N$, prin urmare x^m este nulpotent. Din $(x^m)^k = 0 \Rightarrow x \in N$, deci $\hat{x} = \hat{0}$. ■

Idealul N s.n. nilradicalul inelului R . De exemplu, nilradicalul inelului \mathbb{Z}_{64} este alcătuit din clasele întregilor multiplii de 2: $N = 2\mathbb{Z}_{64} = \{\hat{0}, \hat{2}, \dots, \hat{62}\}$. Inelul factor $\mathbb{Z}_{64}/N = \{\bar{0}, \bar{1}\}$, unde $\bar{i} = \{\hat{2m+i} \mid 0 \leq m \leq 31\}$. și $\bar{0} = N$.

(5) EXERCITIU. Fie x un element nulpotent în inelul R . Atunci $1+x$ este inversabil în R ; mai general, suma unui nulpotent cu un elem. inversabil este inversabil.

2.2. Ideal prim. Fie R un inel cu divizori ai lui zero (există $a, b \in R$, $a \neq 0$, $b \neq 0$, dar $ab = 0$). Se afiră că proprietatea să există un ideal $I \subseteq R$ cu \hat{x} în inel factor R/I și fie fără divizori ai lui zero (altfel spus, R/I să fie domeniu de integritate sau inel integral). Conditia R/I inel integral se traduce prin implicația $(a+I)(b+I) \subseteq I \Rightarrow a+I = I$ sau $b+I = I$, echivalentă cu implicația $(ab \in I \Rightarrow a \in I \text{ sau } b \in I)$ ori $(a \notin I \text{ și } b \notin I \Rightarrow ab \notin I)$. Cu aceste consideranțe se ajunge la defin. următoare.

(6) DEF. Idealul $P \subset R$ este ideal prim dacă $P \neq R$ și dacă $xy \in P \Rightarrow x \in P$ sau $y \in P$.

(7) EXEMPLU. Idealul $n\mathbb{Z} \subseteq \mathbb{Z}$ este prim dacă $n = 0$ sau n este nr. prim.

(8) EXEMPLU. Fie $R = \mathbb{K}[x_1, \dots, x_n]$, unde \mathbb{K} este un corp comutativ. Dacă $f \in R$ este un polinom ireductibil, atunci idealul $\langle f \rangle$ este prim. De exemplu, polinomul $f = x^2 - 2 \in \mathbb{Q}[x]$ este ireductibil peste \mathbb{Q} , de asemenea $f = x^2 + 2x + 4 \in \mathbb{R}[x]$ este ireductibil peste \mathbb{R} . În fine, $f = x^3 + x^2 + x + 1 \in \mathbb{Z}_5[x]$ e ireductibil.

(9) TEOR. Pentru idealul $P \subset R$ urmării afirmații sunt echivalente.

(i) P este ideal prim;

(ii) Inelul factor R/P este domeniu de integritate.

Dem. (i) \Rightarrow (ii). Fie $\hat{a} = a + P$ și $\hat{b} = b + P$ două elemente din R/P a.s. $\hat{a} \cdot \hat{b} = \hat{0}$, altfel spus $(a+P)(b+P) = P$. Atunci $ab \in P$, deci $a \in P$ sau $b \in P$. Deci $\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$.

(ii) \Rightarrow (i). În primul rând, $P \neq R$ deoarece dacă $P = R$, atunci $R/P = \langle \hat{0} \rangle$.

Fie $a, b \in R$ a.s. $ab \in P$. Atunci $\hat{a} \cdot \hat{b} = \hat{0}$. Fiindcă R/P este domeniu de integritate rezultă $\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$, altfel spus, $a \in P$ sau $b \in P$. ■

2.3 Ideal maximal. Am văzut că, în general, într-un inel există elemente neînversabile. Să cercetăm ce condiții trebuie să îndeplinească un ideal $I \subset R$ pt. ca inelul factor R/I să fie corp. În primul rând, ca și în cazul idealurilor prime, $I \neq R$; altfel, $\hat{1} = \hat{0}$. Fie $\hat{a} \neq \hat{0}$. Atunci $\exists \hat{b} \neq \hat{1}$ s.t. $\hat{a} \cdot \hat{b} = \hat{1}$. Rezultă că dacă $a \notin I$, atunci există $b \notin I$ s.t. $1-ab \in I$, de unde $1 \in \langle a \rangle + I$. În definitiv, $R = \langle a \rangle + I$, egalitate pe care o interpretăm astfel: orice ideal care conține strict pe I coincide cu inelul R . Se ajunge la defin. următoare.

(10) DEF. Fie R un inel comutativ și unitar. Idealul $M \subset R$ s.m. maximal dacă $M \neq R$ și nu există niciun ideal I s.t. $M \subset I \subset R$ (ineluziuni stricte).

(11) EXEMPLU. Idealul $\langle 5 \rangle$ este maximal în \mathbb{Z} ; idealul $\langle 10 \rangle$ nu este maximal deoarece $\langle 10 \rangle \subset \langle 5 \rangle \subset \mathbb{Z}$.

(12) PROP. Într-un inel comutativ unitar, idealul $\langle 0 \rangle$ este maximal dacă și numai dacă R este corp.

Dem. Fie R un corp și fie $I \subset R$ un ideal, $\langle 0 \rangle \subset I \subset R$. Dacă $a \in I$, $a \neq 0$, atunci $a^{-1}a \in I$, deci $1 \in I$. Învers, presupunem că $\langle 0 \rangle$ este maximal și fie $a \in R$, $a \neq 0$. Deoarece $\langle a \rangle = R$ rezultă că $1 \in \langle a \rangle$, deci $\exists b \in R$ a.s. $1 = ab$. ■

(13) TEOR. Pentru idealul $M \subset R$ urmt. afirmații sunt echivalente:

- (i) M este maximal;
- (ii) R/M este corp.

Dem. (i) \Rightarrow (ii). Fie $\hat{a} + \hat{\delta}$ în inclusul factor R/M . Atunci $a \notin M$ și idealul $M + \langle a \rangle = R$, deci $M \subset M + \langle a \rangle$ (inclusiune strictă). Înțeles că $1 \in R$ se scrie $1 = m + a \cdot r$, unde $m \in M$ și $r \in R$. Dacă $1 - ar \in M \Rightarrow \hat{r} = \hat{a}^{-1}$, respectiv că \hat{a} este inversabil.

(ii) \Rightarrow (i). Restulă din consil. făcute la începutul paragrafului 2.3. ■

(14) COR. Orice ideal maximal este prim.

Dem. Dacă $M \subset R$ este maximal, atunci R/M este corp, prin urmare R/M este domeniu de integritate. ■

(15) APLICATIE. Fie K un corp comutativ și $K[x]$ inclusul integrul al polinomilor cu coef. în K . Dacă $f \in K[x]$ este un polinom ireductibil, atunci

(a) $P = \langle f \rangle$ este ideal prim în $K[x]$.

(b) Fie $\tilde{K} := K[x]/\langle f \rangle$. Polinomul $f \in \tilde{K}[y]$ are cel puțin o radicare în \tilde{K} , anume \hat{x} .

(16) APLICATIE (se schimbă de construcție a corpului C al nr. complexe).

(a) Cond. ca polin. $ax^2 + bx + c \in R[x]$, $a \neq 0$ să nu aibă răd. reale (adică, $\Delta < 0$) este echiv. cu cond. ca polin. $x^2 + 1 \in R[x]$ să nu aibă rădăcini reale.

(b) Idealul $\langle x^2 + 1 \rangle$ este maximal în $R[x]$.

(c) $C := R[x]/\langle x^2 + 1 \rangle$ este un corp în care polinomul $y^2 + 1 \in C[y]$ are cel puțin o radicare.

Soluție (a) $ax^2 + bx + c = a \left[\left(x + \frac{b}{2a} \right)^2 - \frac{\Delta}{4a^2} \right]$, $\Delta = b^2 - 4ac$. Apoi,

$$\Delta < 0 \Leftrightarrow ax^2 + bx + c = a \left[\left(x + \frac{b}{2a} \right)^2 + \left(\sqrt{\frac{-\Delta}{2a}} \right)^2 \right] = \frac{a}{\left(\sqrt{\frac{-\Delta}{2a}} \right)^2} \left[\left(\frac{x + \frac{b}{2a}}{\sqrt{\frac{-\Delta}{2a}}} \right)^2 + 1 \right]$$

(b) Fie $M = \langle x^2 + 1 \rangle$ și fie $M \subseteq I \subseteq R[x]$. Presupunem $I + M \neq I$, fie $f \in I$. Avem $f = (x^2 + 1)q + ax + b$, unde $ax + b \neq 0$ ($\Leftrightarrow |a| + |b| \neq 0$). Dacă $a = 0$, atunci $b \neq 0$ și $b \in I \Rightarrow b \cdot \frac{1}{b} \in I$, deci $I = R[x]$. Dacă $a \neq 0$, atunci $a(x + \frac{b}{a}) \in I \Rightarrow x + b' \in I$, unde $b' = \frac{b}{a}$. Mai departe, $x(x + b') \in I \Rightarrow (x^2 + 1) + b'x - 1 \in I \Rightarrow b'x - 1 \in I$. În fine, din $x + b' \in I$ și $b'x - 1 \in I \Rightarrow b'^2 + 1 \in I$, resp. $1 \in I$.

Dacă, în ambele cazuri, $a = 0$ sau $c = 0$, rezultă $\mathbb{I} = \mathbb{R}[x]$.

(c) Se notează cu \hat{x} clasa polinomului $x \in \mathbb{R}(x)$. Atunci $\hat{x}^2 + \hat{i} = \hat{0}$ în \mathbb{C} . Se identifică elementele corpului \mathbb{C} . Un sistem complet de reprezentanțe ai polinoamelor din inelul factor $\mathbb{R}[x]/\langle x^2 + i \rangle$ este alcătuit din polinoamele $a + bx \in \mathbb{R}[x]$, deci $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Aplicația $r \mapsto \hat{r}$, $\mathbb{R} \rightarrow \mathbb{C}$ este morfism injectiv de corpuri, motiv pt. că identificăm nr. reale r cu clasa \hat{r} din \mathbb{C} . Dacă urmăreștem, elem. $\hat{a} + \hat{b} \cdot \hat{x}$ îl scriem $a + b \hat{x}$. Adunarea și înmulțirea din \mathbb{C} sunt operațiile obișnuite ca clase:

$$(a+b\hat{x})+(c+d\hat{x}) = \underbrace{(a+c)+(b+d)\hat{x}},$$

$$(a+b\hat{x}) \cdot (c+d\hat{x}) = (a+b\hat{x}) \underbrace{(c+d\hat{x})}_{= ac+(ad+bc)\hat{x}+bd\hat{x}^2} = \underbrace{ac+(ad+bc)\hat{x}}_{= (a+b)(c+d)} + bd\hat{x}^2, \text{ de unde } \hat{x}^2 = -1.$$

Cu notația $i := \hat{x}$, obținem că $\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R} \text{ și } i^2 = -1\}$.

(17) EXERCITIU. Corpul \mathbb{C} construit în Aplicație 16 este izomorf cu corpul $(\mathbb{R} \times \mathbb{R}, +, \cdot)$, unde

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (ac, bd)$$

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac - bd, ad + bc)$$

Nr. real r poate fi identificat cu paranteza $(r, 0)$. Aici, $(0, 1) \cdot (0, 1) = (-1, 0)$, deci $(0, 1)^2 + 1 = 0$.

(18) EXERCITIU. Identificați elementele inelilor factor $\mathbb{R}/\langle 0 \rangle$ și \mathbb{R}/R și izomorfismele $\mathbb{R}/\langle 0 \rangle \cong \mathbb{R}$ și $\mathbb{R}/R \cong \langle 0 \rangle$

(19) EXERCITIU. Arătați că polinomul $ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$, și $\Delta = b^2 - 4ac < 0$ are rădăcini în corpul \mathbb{C} și că formula $x = \frac{-b \pm \sqrt{\Delta}}{2a}$ funcționează și în acest caz cu convenția $\sqrt{-1} = i$.

(20) EXERCITIU. Idealele maxime ale lui \mathbb{Z} sunt de forme $p\mathbb{Z}$, p prim.

(21) EXERCITIU. Arătați că $\mathbb{Z}[i]/\langle 1+i \rangle \cong \mathbb{Z}_2$.

Ind. $1+i \equiv 0 \pmod{1+i}$ și $i \equiv -1 \pmod{1+i}$. Din $\widehat{1+i} = \widehat{0}$ rezultă $\widehat{(1+i)(1-i)} = \widehat{0}$, deci $\widehat{2} = \widehat{0}$. În consecință, $\widehat{a+bi} = \widehat{a} + \widehat{b} \cdot \widehat{i} = \widehat{a} \pmod{2} - \widehat{b} \pmod{2} \in \{\widehat{0}, \widehat{1}, \widehat{-1}\}$. Dar $\widehat{-1} = \widehat{i}$ de unde $\widehat{2} = \widehat{0}$. În definitie, $\mathbb{Z}[i]/\langle 1+i \rangle = \{\widehat{0}, \widehat{1}\}$ împreună cu operațiile:

+	$\widehat{0}$	\widehat{i}
$\widehat{0}$	$\widehat{0}$	\widehat{i}
\widehat{i}	\widehat{i}	$\widehat{0}$

*	$\widehat{0}$	\widehat{i}
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
\widehat{i}	\widehat{i}	$\widehat{1}$

Transferuri de proprietăți între inel și inclus factor

În continuare, R este un inel comutativ unitar.

(1) PROP. Fie $I \subseteq R$ un ideal și fie $\varphi: R \rightarrow R/I$ morfismul surjectiv care asociază fiecărui element $x \in R$ clasa $[x] = x + I$ în inclus factor. Există o corespondență bijectivă ce conservă incluziunea între idealele J ale lui R ce conțin pe I și idealele J' ale lui R/I date de $J' = \varphi^{-1}(J)$.

Dem. Fie J mult. idealelor în R care conține pe I și J' mult. idealelor lui R/I .

Dacă $j' \in J'$, atunci $j = \varphi^{-1}(j') \in J$: într-adevăr, fie $x, y \in j$. Din $\varphi(x), \varphi(y) \in j'$ rezultă $\varphi(x-y) \in j'$, ceea ce implica $x-y \in \varphi^{-1}(j') = J$. De asemenea, dacă $r \in R$, atunci $\varphi(rx) = \varphi(r)\varphi(x) \in j'$, deci $rx \in \varphi^{-1}(j')$. Învers, dacă $j \subseteq R$ ideal care conține pe I , at. $J' = \varphi(j) \in J$. Într-adevăr, fie $\hat{x}, \hat{y} \in J'$, respectiv $\hat{x} = x + I, \hat{y} = y + I$, unde $x, y \in j$. Atunci, $x-y \in j \Rightarrow \varphi(x-y) = \hat{x}-\hat{y} = \hat{x}-\hat{y} = (x+I)-(y+I) = x-y+I \in J'$. De asemenea, dacă $\hat{r} = r+I \in R/I$, atunci $\hat{r}\hat{x} = \hat{r}x = rx+I \in J'$ devenind $rx \in j$.

Corespondențele $\varphi: J \rightarrow J'$, $\varphi: J \mapsto \varphi(J)$ și $\varphi: J' \rightarrow J$, $\varphi: j' \mapsto \varphi^{-1}(j')$ sunt inverse una către alta $\varphi^{-1}(\varphi(j)) = j$ și $\varphi(\varphi^{-1}(j')) = j'$, fapt ce confirmă coresp. bijectivă dintre cele două familii de ideale. ■

OBS. Aplic. φ din Prop. 1 s. n. morfismul canonic al lui R în R/I .

Propoziția următoare stabilește o corespondență mai specială între idealele a două inele.

(2) PROP. Fie $\varphi: R \rightarrow S$ un morfism de inele.

(i) Dacă $J \subseteq S$ este un ideal prim, at. $\varphi^{-1}(J)$ este ideal prim în R.

(ii) Dacă φ este morfism surjectiv și P este un ideal prim ce conține $\text{Ker } \varphi$, atunci $P' = \varphi(P)$ este un ideal prim în S.

Dem (i) Fie J' ideal prim în S. Cât timpă verifică faptul că $J = \varphi^{-1}(J')$ este ideal în R. Arătăm că J este prim. Fie $a, b \in R$ a.s. $ab \in J$. Atunci $\varphi(ab) \in J'$ $\Rightarrow \varphi(a) \cdot \varphi(b) \in J' \Rightarrow \varphi(a) \in J'$ sau $\varphi(b) \in J' \Rightarrow a \in \varphi^{-1}(J')$ sau $b \in \varphi^{-1}(J')$.

Condiția $J \neq S$ este îndeplinită pt. că $J \neq J' \Rightarrow \varphi^{-1}(J') \neq \varphi^{-1}(J_s)$.

(ii) Fie $P \subseteq R$ ideal prim a.s. $P \supseteq \text{Ker } \varphi$. Cât timpă verifică faptul că $P' = \varphi(P)$ este un ideal în S. Arătăm că P' este prim: fie $a, b \in S$ a.s. $a \cdot b \in P'$.

Premparam $a' = \varphi(a)$, $b' = \varphi(b)$, unde $a, b \in R$. Atunci, $\varphi(ab) = a'b' \in P' = \varphi(P) \Rightarrow \exists p \in P$ s.t. $p(ab) = \varphi(p)$. Rezulta că $ab - p = e$, cu $e \in \text{Ker } \varphi$. Deoarece $\text{Ker } \varphi \subseteq P$ se obtine $ab \in P$, de unde $a \in P$ sau $b \in P$. Urmează că $a' = \varphi(a) \in P'$ și $b' = \varphi(b) \in P'$. Se arată că $P' \neq S$: avem $1_R \notin P$. Dacă, prin absurd, $P' = S$, atunci $1_S = \varphi(p)$, unde $p \in P$. Obținem $1_S = \varphi(p) \Rightarrow 1_S = \varphi(p \cdot 1_R) = \varphi(p) \cdot \varphi(1_R) = \varphi(1_R)$. Din $\varphi(p) = \varphi(1_R) \Rightarrow 1_R - p \in \text{Ker } \varphi \Rightarrow 1_R - p \in P \Rightarrow 1_R \in P$, contradicție.

(3) COR. Fie $I \subset R$ un ideal și fie $\varphi: R \rightarrow R/I$ morfismul surjectiv care asociază fiecărui element $x \in R$ clasa sa $\hat{x} = x + I$ din R/I . Atunci există o corespondență bijectivă cu privirea inclusiunii între idealele prime din R ce conțin pe I și idealele prime din R/I , date de aplicațiile inverse $I \in \mathcal{J}(R) \longleftrightarrow \varphi(I) \quad ; \quad J' \in \mathcal{J}(R/I) \longleftrightarrow \varphi^{-1}(J')$.

(4) COR. Idealele prime ale inelului \mathbb{Z}_n , $n > 1$ sunt de forma $\hat{p}\mathbb{Z}_n$, unde p este un nr. prim care divide pe n .

Dem. Aplic. canonică $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ este surjectivă, iar idealele prime din \mathbb{Z} sunt generate de nr. prime, adică de forma $p\mathbb{Z}$, unde p este prim. Atunci $\pi(p\mathbb{Z}) = \pi(p) \cdot \pi(\mathbb{Z}) = \hat{p}\mathbb{Z}_n$. $\text{Ker } \pi = n\mathbb{Z}$ deoarece $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Condiția ca $p\mathbb{Z} \supseteq n\mathbb{Z}$ înseamnă $n \in p\mathbb{Z}$, respectiv $p | n$. ■

Corolarul 3 are un corespondent similar pentru idealele maximale. Mai precis, avem propoz. următoare.

(5) PROP. Fie $\varphi: R \rightarrow S$ un morfism surjectiv de inele.

- (i) Dacă $M' \subset S$ este ideal maximal, atunci $M = \varphi^{-1}(M')$ este ideal maximal în R .
- (ii) Dacă M este ideal maximal în R și $\text{Ker } \varphi \subseteq M$, atunci $M' = \varphi(M)$ este ideal maximal în S .

Dem. Din Prop. 1, există o coresp. bijectivă între mulțimile ordonate ale idealelor lui S și idealelor lui R care conțin pe $\text{Ker } \varphi$. Atunci, elementele maximale din cele două mulțimi se corespund. ■

Idealele prime și idealele maxime joacă un rol important în studiul inelului. Printre altele, semnificația nilradicalului N este intersecția tuturor idealelor prime. Intersecția idealelor maxime este, de asemenea, un ideal important numit radicalul Jacobson.

În ultima parte ale acestei lecții evidențiem cîteva proprietăți ale acestor tipuri de ideale.

- (6) PROP. (i) Dacă P_1, \dots, P_n sunt ideale prime s.a.z. idealul $I = \bigcup_{i=1}^n P_i$, atunci există un i s.a.z. $I \subseteq P_i$.
(ii) Fie P un ideal prim și fie I_1, \dots, I_n ideale s.a.z. $P \supseteq \bigcap_{i=1}^n I_i$. Atunci există un i s.c. $P \supseteq I_i$. Dacă $P = \bigcap_{i=1}^n I_i$, at. există i s.a.z. $P = I_i$.

Dem (i) Vom dem. prin inducție după n

$$I \not\subseteq P_j \quad (1 \leq j \leq n) \Rightarrow I \not\subseteq \bigcup_{j=1}^n P_j.$$

Prop. este evident adevărată pt. $n=1$. Fie $n > 1$ și pres. prop. adev. pt. $n-1$. Pt. fiecare i fixat există un element $x_i \in I$, dar $x_i \notin P_j$, $\forall j \neq i$. Cu ipot. de inducție, $x_i \notin \bigcup_{j \neq i} P_j$. Dacă există un i pt care $x_i \notin P_i$, at. $x_i \notin \bigcup_{j=1}^n P_j$. Dacă nu, pt totuși i evenim $x_i \in P_i$ considerăm elem

$$y = \sum_{j=1}^n x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n.$$

Pentru o parte, $y \in I$, dar pe de altă parte $y \notin P_i$, $\forall 1 \leq i \leq n$, deoarece $x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n \in P_i \Rightarrow$ cel puțin un $x_j \in P_i$, $j \neq i$, imposibil.

(ii) Pres., prim absurd, că $P \not\supseteq I_i$, $\forall 1 \leq i \leq n$. Pt. fiecare i există $x_i \in I_i$, dar $x_i \notin P$. Rezultă că $\prod x_i \in \prod I_i \subseteq \bigcap I_i$. Deoarece P este prim avem că $\prod x_i \notin P$. Adăugăm, $P \not\supseteq \bigcap I_i$, contradiction cu ipoteza. În final ducem $P = \bigcap I_i$, at. $P \subseteq I_i$, deci $P = I_i$ pt. un i , $1 \leq i \leq n$. ■

(7) PROP. Într-un inel comutativ și unitar R , idealul $\langle 0 \rangle$ este maximal dacă și numai dacă R este corp.

Dem, exercițiu. ■

(8) TEOR. Într-un inel comutativ unitar cu 1+0 orice ideal este conținut într-un ideal maximal.

Dem. Se folosește lema lui Zorn cf. cîrceea decesă A este o multime parțialordonată în care orice parte totalordonată are un majorant în A, atunci A conține un element maximal.

Fie R inel și fie $I \subset R$ un ideal. Fie A multimea tuturor idealelor din R și diferențe de R ce conțin pe I. (A, \subseteq) este parțialordonat cu incluziunea. Fie $(I_j)_{j \in J}$ o multime totalordonată de ideale din A. Fie $I' = \bigcup I_j$. Afirmația I' este ideal din A: într-adevăr, dacă $x, y \in I'$, atunci există $i, k \in J$ s.t. $x \in I_i, y \in I_k$. A fiind totalordonat avem $I_i \subseteq I_k$ sau $I_k \subseteq I_i$. Corespunzător, $x - y \in I_i$ sau $x - y \in I_k$. Prin urmare, $x - y \in I'$. Dacă $x \in I'$, atunci $rx \in I_i \subseteq I'$. În fine, $I' \neq R$ deoarece în caz contrar, $1 \in I'$ și atunci $\exists j \in J$ s.t. $1 \in I_j$, deci $R = I_j$. Multimea A astfel definită îndeplinește condițiile lemei lui Zorn. Rezultă că A are un element maximal; acesta este un ideal maximal ce conține pe I. ■

(9) TEOR. În orice inel comutativ unitar nemul există ideale maximale.

(10) TEOR (lema chineză a resturilor-formă în inelul \mathbb{Z}). Fie $m_1, \dots, m_n \in \mathbb{Z}^*$ astfel că $(m_i, m_j) = 1$ pentru toți $i \neq j$ din $\{1, 2, \dots, n\}$. Dacă b_1, \dots, b_n sunt nr. întregi oricare, atunci sistemul de n congruențe

$$x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_n \pmod{m_n}$$

are o soluție unică determinată modulo $m_1 m_2 \dots m_n$.

Dem. Notăm $m = m_1 m_2 \dots m_n$ și $m_i = \frac{m}{m_i} = m_1 \dots \hat{m}_i \dots m_n$. Din $(m_i, m_j) = 1$ rezultă că există întregi u_i, v_i s.t. $u_i m_i + v_i m_j = 1$. Punem $e_i = v_i m_i$. Atunci $e_i \equiv 1 \pmod{m_i}$, deci $b_i e_i \equiv b_i \pmod{m_i}$. În plus, $e_i \equiv 0 \pmod{m_j}$ pentru toți $j \neq i$. Fie $x = b_1 e_1 + b_2 e_2 + \dots + b_n e_n$. Integru x este o soluție a sistemului de congruențe dat. Dacă y este o altă soluție, atunci din $x \equiv y \pmod{m_i}$ rezultă $m_i | x - y$, $\forall i \in \{1, 2, \dots, n\}$ deci $m_1 \dots m_n | x - y$. Deci, $x \equiv y \pmod{m}$.

(11) EXEMPLU. Să rezolvăm sistemul de congruențe

$$x \equiv 1 \pmod{2}, \quad x \equiv 4 \pmod{3} \text{ și } x \equiv 2 \pmod{5}.$$

Sol. Aici $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ și $M = 30$. Corespondent, $n_1 = 15$, $n_2 = 10$ și $n_3 = 6$. Ec. $u_1 \cdot 2 + v_1 \cdot 15 = 1$ are sol. pe $u_1 = 23$, $v_1 = -3$, deci putem scrie $e_1 = n_1 \vartheta_1 = -45$. Ec. $u_2 \cdot 3 + v_2 \cdot 10 = 1$ are sol. pe $u_2 = 7$ și $v_2 = -2$; deci $e_2 = n_2 \vartheta_2 = -20$. În schimb, ec. $u_3 \cdot 5 + v_3 \cdot 6 = 1$ are soluția $u_3 = -1$, $v_3 = 1$, de unde $e_3 = n_3 \vartheta_3 = 6$. Am obținut sol. $x = b_1 e_1 + b_2 e_2 + b_3 e_3 = -45 - 80 + 12 = -113$ și $y = -113 + 4M = 7$. Rezultă că mult. soluților este $\{7 + 30k \mid k \in \mathbb{Z}\}$.

(12) TEOR (lemea chineză a resturilor-formă generală). Fie I_1, \dots, I_n ideale în inelul R cu condiție $R^2 + I_i = R$, $\forall i = 1, \dots, n$ și $I_i + I_j = R$, $\forall i \neq j$. Dacă $b_1, \dots, b_n \in R$ atunci există $b \in R$ s.a.

$$b \equiv b_i \pmod{I_i}, \quad 1 \leq i \leq n.$$

Mei mult, b este unic determinat prin legea congruențelor modulo idealul $I_1 \cap I_2 \cap \dots \cap I_n$.

Dem. Într-adevăr să observăm că R este inel unitar, astfel că condiția $R^2 + I_i = R$ este satisfăcătoare deoarece $R^2 = R$.

Din $I_1 + I_2 = R$ și $I_1 + I_3 = R$ rezultă că

$$R^2 = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_1 I_2 + I_1 I_3 + I_2 I_3 \subseteq I_1 + I_2 I_3 \subseteq I_1 + I_2 \cap I_3.$$

Atunci, $R = R^2 + I_1 \subseteq I_1 + I_2 \cap I_3$, deci $R = I_1 + I_2 \cap I_3$. Prempunem că

$R = I_1 + I_2 \cap I_3 \cap \dots \cap I_{n-1}$. Dacă ar trebui că $R = I_1 + I_2 \cap I_3 \cap \dots \cap I_n$. Într-adevăr, din

$$R = (I_1 + I_2 \cap \dots \cap I_{n-1}) \cdot (I_1 + I_n) \subseteq I_1 + I_2 \cap \dots \cap I_n$$

se obține că $R = R^2 + I_1 = I_1 + I_2 \cap \dots \cap I_n$. În concluzie, $R = I_1 + \cap_{i=1}^{n-1} I_i$.

În general, $R = I_i + \cap_{k \neq i} I_k$. Pentru fiecare $b_i \in R$ există $a_i \in I_i$ și $r_i \in \cap_{k \neq i} I_k$ a.s. $b_i = a_i + r_i$. Rezultă că

$$b_i \equiv r_i \pmod{I_i} \text{ și } b_i \equiv 0 \pmod{I_k}, \quad \forall k \neq i.$$

Punem $b = r_1 + \dots + r_n$. Atunci, $b \equiv b_i \pmod{I_i}$ și orice i . În schimb, dacă $c \in R$ este o altă soluție, astfel că $c \equiv b_i \pmod{I_i}$, $\forall i$ rezultă că $c \equiv b \pmod{I_i}$, $\forall i$. În urmare, $c - b \in I_i$ și $1 \leq i \leq n$, de unde $c - b \in \cap_{i=1}^n I_i$. ■

(13) EXERCITIU. Demonstrați Teor. 10 folosind demonstrația Teoremei 12.

(14) EXERCITIU. Fie $R \neq 0$ un inel. Atunci următoarele sunt echivalente

- (i) R este c.p.;
- (ii) singurile ideale în R sunt $\langle 0 \rangle$ și $\langle 1 \rangle = R$;
- (iii) orice morfism de inele $R \rightarrow S$ este injectiv.

Ind. Se arată $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$. ■

(15) EXERCITIU. Demonstrați echivalența: M ideal maximal în $R \Leftrightarrow R/M$ este c.p., folosind Exemplul 14 și Prop. 1.

(16) EXERCITIU. Construiți inelul $\mathbb{Z}[i]/\langle 2 \rangle$.

Ind. $\mathbb{Z}[i]/\langle 2 \rangle$ este format din 4 clase de reprezentanți: $0, 1, i, 1+i$.

Tablile adunării și înmulțirii din inelul $R = \mathbb{Z}[i]/\langle 2 \rangle = \{\hat{0}, \hat{1}, \hat{i}, \hat{1+i}\}$ permit identificarea unui izomorfism de inele unitare $R \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$.

(17) EXERCITIU. Se se arată că $\mathbb{Z}[i]/\langle 2 \rangle \cong \mathbb{Z}_2[x]/\langle x^2+1 \rangle$.

(18) EXERCITIU. Construiți inelul: $\mathbb{Z}[i]/\langle 1+2i \rangle$.

Ind. $(1+2i)(i-2i) \equiv 0 \pmod{\langle 1+2i \rangle} \Rightarrow 5 \equiv 0 \pmod{\langle 1+2i \rangle}$. Se arată că $0 + \varepsilon i, 1 + \varepsilon i, 2 + \varepsilon i, 3 + \varepsilon i \not\sim 4 + \varepsilon i$, unde $\varepsilon \in \{0, 1\}$ constituie un sistem complet de reprezentanți în $\mathbb{Z}[i]/\langle 1+2i \rangle$.

L8 - AHEXA

(i) OBS. (în legătură cu Lem. Prop. 1)

(ii) În general, dacă $\varphi: R \rightarrow S$ este o funcție între două mulțimi avem

$$\varphi^{-1}(\varphi(J)) = J, \forall J \subseteq R \quad (\varphi: R \rightarrow R, J = [0, 2]: \varphi^{-1}(\varphi(J)) = [-2, 2] \neq J)$$

$$\text{și } \varphi(\varphi^{-1}(J')) = J' \cap \varphi(R), \forall J' \subseteq S. \quad (\varphi: R \rightarrow R, \varphi(x) = [x]: \varphi(\varphi^{-1}([0, 2])) \subseteq [0, 2])$$

(iii) În cnd. Prop. 1 avem $\varphi(\varphi^{-1}(J')) = J'$ deoarece $\varphi: R \rightarrow R$ și este surjectivă, iar $\varphi^{-1}(\varphi(J)) = J$ deoarece J este ideal în R .

(2) OBS. (să detaliereze a dem. Prop. 6.(i))

$$(i) I \notin P_j, \forall j = 1, n \Rightarrow I \notin \bigcup_{j=1}^n P_j$$

Dem prin inducție după n . Pres. afirmația să se pt. $n-1$ și să dem. pt. n .

Există un element, notat $x_1 \in I$ s.t. x_1 nu aparține niciunui din idealele P_1, \dots, P_n , deoarece altfel $\forall x \in I$ aparține cel puțin unei dintre idealele P_1, \dots, P_n ; în acest caz, $x \in \bigcup_{j=1}^n P_j$ și cu ip. de inducție $\exists j \in \{2, \dots, n\}$ s.t. $I \subseteq P_j$. În mod analog, există un element, notat $x_2 \in I$ care nu aparține niciunui din idealele P_1, P_2, \dots, P_n etc. Astăzi, pt. fiecare $i \in \{1, 2, \dots, n\}$ există $x_i \in I$ care nu aparține niciunui din idealele P_j , $j \neq i$. Cu ipoteza de inducție, $x_i \notin \bigcup_{j=1}^i P_j$. Dacă vrem $x_i \notin$ nici un P_i , atunci $x_i \notin \bigcup_{j=1}^{i-1} P_j$ și deci $I \notin \bigcup_{j=1}^{i-1} P_j$. În sf, dacă totuși $x_i \in P_i$, elementul

$$y = \sum_{i=1}^{\infty} x_1 \dots x_{i-1} x_{i+1} \dots x_n$$

apartine lui I , deci nu aparține niciunui P_i , deci și în acest caz $I \notin \bigcup_{j=1}^n P_j$.

$$(ii) \prod_{i=1}^n I_i = \left\{ \sum_{\text{finite}} x_1 \dots x_n \mid x_i \in I_i \right\}, \text{ altfel spus, } \prod_{i=1}^n I_i = \langle x_1 \dots x_n \mid x_i \in I_i \rangle.$$

(3) OBS. (în legătură cu lemea lui Zorn). Fie (A, \leq) o mulțime parțial ordonată.

Un element $a \in A$ este maximal dacă pentru orice $c \in A$ care este comparabil cu a avem $c \leq a$; altfel spus, pt. totuși $c \in A$, $a \leq c \Rightarrow a = c$.

Exemplu. \mathbb{Z} cu ordinea usuală nu are elem. maximele.

Exemplu. $S = \{(x, y) \in \mathbb{R}^2 \mid y \leq 0\}$. Definim $(x_1, y_1) \leq (x_2, y_2) \Leftrightarrow x_1 = x_2 \wedge y_1 \leq y_2$. Sunt și infinite de elemente maxime.

1. Caracteristica unui corp.

Fie R un inel comutativ și unitar. Deci există un cel mai mic întreg pozitiv n pentru care $n \cdot 1 = 0$, în sensul $\underbrace{1 + 1 + \dots + 1}_{\text{de } n \text{ ori}} = 0$, atunci se spune că R are caracteristica n . Dacă nu există un astfel de n , atunci se spune că R are caracteristica zero. Se scrie $\text{char } R = n$.

1. PROP. Fie R un inel unitar de caracteristică $n > 0$.

- (a) Aplicația $m \mapsto m1$, $\mathbb{Z} \rightarrow R$ este un morfism de inele cu nucleul $\langle n \rangle = \{km \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.
- (b) Dacă R este domeniu, atunci n este număr prim.

DIM. (b) Dacă $n = rs$, cu $1 < r < n$, $1 < s < n$, atunci $0 = n1 = \underbrace{r1}_R \underbrace{s1}_R = \underbrace{1_2 + 1_2 + \dots + 1_2}_{\text{de } r \text{ ori}} + \underbrace{1_2 + \dots + 1_2}_{\text{de } s \text{ ori}} = (1_2 + \dots + 1_2)(1_2 + \dots + 1_2) = (r1_R)(s1_R)$. R domeniu $\Rightarrow r1_R = 0$ sau $s1_R = 0$, contradicție cu alegerea lui n . \blacksquare

Holoteca de caracteristică se folosește mai des în cazul în care R este un corp. Pentru a pune mai bine în evidență semnificația noțiunii de caracteristică a unui corp, începem cu o scurtă prezentare.

2. PROP. Dacă R este un inel comutativ unitar cu $1 \neq 0$, at. U.A.E. :

- (a) R corp,
- (b) Orice morfism nuanță de inele $\varphi: R \rightarrow S$ este monomorfism.

DIM. a) \Rightarrow b). Dacă R este corp, at. singurile ideale sunt $\langle 0 \rangle$ și $\langle 1 \rangle = R$.

Dacă, $\text{Ker } \varphi = \langle 0 \rangle$ sau $\text{Ker } \varphi = R$. Varianta $\text{Ker } \varphi = R$ este imposibilă deoarece înseamnă că $\varphi = 0$.

b) \Rightarrow a). Presupunem că R nu e corp și fie $0 \subsetneq I \subsetneq R$ un ideal. Morfismul canonic $\pi: R \rightarrow R/I$ are $\text{Ker } \pi = I$, fapt ce înseamnă că π nu este injectiv. \blacksquare

3. DEF. O submultime nevidă k a unui corp K s.n. subcorp al lui K dacă operațiile algebrice de pe K induc pe k operații algebrice înpreună cu care k este corp.

4. PROP. Fie K un corp și $k \neq \emptyset$ o submultime a lui K. V.A.T.:

(a) k subcorp al lui K.

(b) Oricare ar fi $x, y \in k$ avem $x+y \in k$, iar dacă $y \neq 0$, atunci $xy^{-1} \in k$.

Dem. exercițiu.

5. PROP. Fie K un corp.

(a) Dacă $\text{char } K = 0$, atunci K conține un subcorp izomorf cu corpul \mathbb{Q} al numerelor rationale.

(b) Dacă $\text{char } K = p$, p prim, atunci K conține un subcorp izomorf cu corpul \mathbb{Z}_p .

$$i: m \longmapsto m \cdot \zeta_p$$

Dem. Fie $i: \mathbb{Z} \rightarrow K$ morfismul unită de inele. Atunci $\text{Ker } i = n\mathbb{Z}$, unde $n \geq 0$.

(a) Dacă $n=0$, at. i este monomorfism și i se extinde la un morfism injectiv unic $j: \mathbb{Q} \rightarrow K$, punând $j\left(\frac{m}{n}\right) := i(m) \cdot (i(n))^{-1}$. Atunci, $j(\mathbb{Q}) \subseteq K$ este un corp izomorf cu \mathbb{Q} .

(b) Dacă $n > 0$, atunci $n=p$, p prim. Aici, $\text{Ker } i = p\mathbb{Z}$, iar $i(\mathbb{Z}) \subseteq K$ este un grup izomorf cu grupul aditiv \mathbb{Z}_p . i se extinde la un morfism injectiv unic de corpuri $j: \mathbb{Z}_p \rightarrow K$.

6. PROP. Corpurile \mathbb{Q} și \mathbb{Z}_p , cu p număr prim nu conțin subcorpuri proprii și sunt izomorfe.

Dem. Fie $K \subseteq \mathbb{Q}$ un subcorp al lui \mathbb{Q} . Atunci, $\frac{1}{n} \in K \Rightarrow m \in K, \forall m \in \mathbb{Z}$ și, deci, $n^k \in K$ pentru toți $n \neq 0$. Deci, $\frac{m}{n} \in K, \forall \frac{m}{n} \in \mathbb{Q}$.

Corpurile \mathbb{Q} și \mathbb{Z}_p s.n. corpuri prime devințe, pe de o parte, nu conțin subcorpuri proprii. În cealaltă parte, orice corp K conține un subcorp izomorf, fie că $\text{char } K = 0$, fie că $\text{char } K = p$.

2. Inele de fractii. Corpul de fractii al unui domeniu.

Inele de fractii se construiesc după modelul cunoscut al construcției lui \mathbb{Q} din inelul \mathbb{Z} . După cum sugerează denumirea, aceste inele conțin fractii care se pot forma cu două elemente $r, s \in S$ din inelul R . În general, fractia $\frac{r}{s}$ nu coincide cu r/s , așa cum suntem obișnuiti în inelul de fractii \mathbb{Q} al lui \mathbb{Z} . Însă, atunci când inelul de fractii este corp are loc egalitatea $\frac{r}{s} = r/s$.

Fie R un inel comutativ unitar. O mulțime nevidată S a lui R s.m. sistem multiplicativ (sau \mathbb{S}) și scriem s.m.c. dacă $a, b \in S \Rightarrow ab \in S$.

3. EXEMPLE. În divizorii lui zero intr-un inel nemulunit formeză un s.m.i. Dacă R este domeniu, atunci $S = R \setminus \{0\}$ este un s.m.i. Mulțimea unităților unui inel este un s.m.i. Dacă P este ideal prim în R , atunci $S = R \setminus P$ este un s.m.i.

Fie S un s.m.i. în R . Pe produsul cartezian $R \times S$ se introduce următoarele relație binară:

$$(r, s) \sim (r', s') \text{ dacă } \exists t \in S \text{ s.t. } t(r's' - rs) = 0. \quad (1)$$

8. PROP. Relația definită de (1) este o rel. de echivalență pe $R \times S$. În plus, dacă R nu are divizori ai lui zero și $0 \notin S$, atunci

$$(r, s) \sim (r', s') \Leftrightarrow rs' = r's. \quad (2)$$

Dem. Exercițiu. ■

Clasa de echivalență a lui $(r, s) \in R \times S$ se notă $\frac{r}{s}$, iar mulțimea tuturor claselor de echivalență se notează R_S sau RS' . Se observă că

- (a) $\frac{r}{s} = \frac{r'}{s}$, dacă $\exists t \in R$ s.t. $t(rs' - r's) = 0$;
- (b) $\frac{tr}{ts} = \frac{r}{s}$, pentru toți $t \in R$ și $s, t \in S$;
- (c) Dacă $0 \in S$, atunci R_S este eluștită dintr-o singură clasă de echivalență.

9. TEOR. Fie S un S.m. și în inclusiv comutativ R și R_S mult. abs. de echiv. ale lui $R \times S$ date de rel. de echiv. (1).

(a) R_S este un inel comutativ unitar cu adunarea și înmulțirea date prin

$$r/s + r'/s' := (rs' + r's)/ss' \quad \text{și} \quad (r/s) \cdot (r'/s') := rr'/ss'.$$

(b) Dacă R este un inel număr fără divizori ai lui zero și $0 \notin S$, atunci R_S este domeniu.

(c) Dacă R este inel număr fără divizori ai lui zero și $S = R \setminus \{0\}$, atunci R_S este un corp (comutativ).

Dem. (a) Vom arăta că adunarea și înmulțirea în R_S sunt bine definite, ceea ce va fi verificat în mod similar la teorema 8. Deși, fie $r/s = r_1/s_1$, $r'/s' = r'_1/s'_1$, și să arătăm că $(rs' + r's)/ss' = (r_1s'_1 + r'_1s_1)/s_1s'_1$. Din ipoteză există $u, v \in S$ s.t.

$$u(rs - r_1s) = 0 \quad \text{și} \quad v(r's' - r'_1s_1) = 0.$$

Atunci

$$uvss'_1(rs' + r's)s_1s'_1 = 0 \quad \text{și} \quad uvss_1(r's'_1 - r'_1s_1)s_1s'_1 = 0,$$

decică

$$uv[(rs' + r's)s_1s'_1 - (r_1s'_1 + r'_1s_1)ss'_1] = 0,$$

care înseamnă că $(rs' + r's)/ss' = (r_1s'_1 + r'_1s_1)/s_1s'_1$. ÎnDEPENDENȚA înmulțirii față de alegerea lui r, s, r', s' și arătă în mod asemănător.

(b) Mai întâi să observăm că $r/s = 0/s$ dacă și numai dacă $r=0$, deci dacă $r=0$. Rezultă că $(r/s) \cdot (r'/s') = 0$ în R_S d. d. m. d. $rr'=0$, respectiv $r=0$ sau $r'=0$. Astfel, R_S este domeniu.

(c) R_S este corp dacă since $r/s \neq 0$ este inversabil. Dacă $r \neq 0$, atunci r/s are sens reciproc s/r . Atunci, $(r/s) \cdot (s/r) = rs/rs' = 1$.

10. OBS. Subliniem că în Teor. 9 inclusiv R nu trebuie să fie neapărat unitar pentru ca R_S să fie unitar. De exemplu, $R = 2\mathbb{Z}$ este neunitar și dacă $S = 2\mathbb{Z} \setminus \{0\} = 2\mathbb{Z}^*$, atunci unitatea lui R_S este reciproc $1/s$, unde $s \in 2\mathbb{Z}^*$.

Inclusiv R_S din Teor. 9 este inelul de fructe al lui R privind S .

În cnd. Teor. 9(c), R_S este corpul de fructe al domeniului R . În acest sens, \mathbb{Q} este corpul de fructe al inclusiv $R = \mathbb{Z}$.

După cum înelul de fractii R_S să a constituit înmulțirea modului construcției lui \mathbb{Q} din \mathbb{Z} , tot astfel elementele înelului R se vor identifica cu fractii din R_S după tiparul $m \longmapsto m/1$, $\mathbb{Z} \rightarrow \mathbb{Q}$.

II. TEOREMA. Fie S un s.m.i. în inelul comutativ R .

(a) Aplicația $\varphi_S : R \rightarrow R_S$ date prin $r \mapsto rS/S$, unde $s \in S$ este arbitrar, este un morfism de inele bine definit și, pentru orice $s \in S$, imaginea sa $\varphi_S(s)$ din R_S este un element inversabil.

(b) Dacă $0 \notin S$ și S nu conține divizori ai lui zero, atunci φ_S este monomorfism. În particular, orice domeniu R poate fi identificat în inelul său de fractii prin monomorfismul $r \mapsto rS/S$.

Dem (a) Dacă $r \in R$, atunci $rS/S = rS'/S'$ pentru orice $S, S' \in S$ deoarece $rSS' - rr'S = 0$, prin urmare, φ_S este bine definit; de asemenea, φ_S este morfism. Dacă $r \in S$, atunci $\varphi_S(r) = r^2/S$ are invers elementul $S/r^2 \in R_S$.

(b) Conditiva $\varphi_S(r) = 0$ înseamnă $rS/S = 0/S$, respectiv $urS^2 = 0$, j.c. un $u \in S$.

Cum S nu are divizori ai lui zero rezultă că $r = 0$.

3. Localizare

Fie R un inel comut. unitar și P un ideal prim în R . Atunci:

(a) $S := R \setminus P$ este un s.m.i. în R , iar inelul de fractii R_S se numește localizarea lui R în P .

(b) Dacă I este ideal în R , atunci $I_P = \{a/s \mid a \in I, s \in S\}$ este ideal în R_P .

(9) TEOR. Fie R un inel comutativ unitar nenuț fiind divizori și lui zero și fie $S = R \setminus \{0\}$. Pe mulțimea $R \times S$ definim rel. binară
 $(r,s) \sim (r',s')$ dacă $r's = r's'$. (1)

(i) Relația \sim este o relație de echivalență pe $R \times S$.

(ii) Fie $\frac{r}{s}$ clase de echivalență a perechii ordonate $(r,s) \in R \times S$ și notăm R_S mulțimea claselor de echivalență. Atunci R_S este un inel comutativ cu adunare și înmulțire definite prin

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'} \quad \text{și} \quad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

(iii) Morfismul $\varphi: R \rightarrow R_S$ dat prin $r \mapsto \frac{r}{1}$ este un morfism injectiv, astfel că izomorfismul $R \cong \varphi(R) \subseteq R_S$ permite identificarea $r = \frac{r}{1}, \forall r \in R$.

(iv) Elementele $\frac{r}{s}, s \neq 0$, sunt inversabile cu inversul $\frac{1}{s} \cdot r$. Altfel spus, elementele nemulte din R sunt inversabile în R_S , via identificarea $r = \frac{r}{1}$.

(v) R_S este un corp, numit corpus de fracții al domeniului R . ■

Dem. Exercițiu. ■

Corpuri. Teoria lui GaloisGeneralități

1. Definții. Considerăm cunoscută platoului de corp..: un inel $\neq 0$ în care orice element nenul este inversabil. În între-un studiu profund care include structura corporilor este utilă propoz. următoare.

(1) PROP. Fie R un inel nenul ($1 \neq 0$). Atunci următoarele sunt echivalente:

(i) R este un corp;

(ii) singurile ideale în R sunt $\langle 0 \rangle$ și $\langle 1 \rangle$;

(iii) orice morfism nenul de inele $\varphi: R \rightarrow S$ (adică, cu dom. de defn. R) este injectiv.

Dem. (i) \Rightarrow (ii). Fie $I \subseteq R$ un ideal. Dacă $I \neq \langle 0 \rangle$, at. există un element nenul $x \in I$.

R fiind corp, x este inversabil. Rezultă $1 = x^{-1} \cdot x \in I$, deci $\langle 1 \rangle \subseteq I$, respectiv $I = \langle 1 \rangle$.

(ii) \Rightarrow (iii). Fie $\varphi: R \rightarrow S$ un morfism de inele. At. $\text{Ker } \varphi$ este un ideal în R .

$\varphi \neq 0 \Rightarrow \text{Ker } \varphi \neq R$, prin urmare $\text{Ker } \varphi = \langle 0 \rangle$. În consecință, φ este injectiv.

(iii) \Rightarrow (i). Fie $x \in R$ un element neinversabil. Atunci $\langle x \rangle \neq \langle 1 \rangle$; Rezultă că morfismul surjectiv $\pi: R \rightarrow R/\langle x \rangle$, $r \mapsto r + \langle x \rangle$ este nenul ($1 + \langle x \rangle \neq \langle x \rangle$). Cf. ipoteza!, π este injectiv, prin urmare $\text{Ker } \pi = 0$. În definitiv, $\langle x \rangle = 0$, deci $x = 0$. ■

(2) DEF. O submulțime nenulă k a unui corp K s.m. subcorp al lui K dacă operațiile algebrice date pe K induc pe k operații algebrice împreună cu care k este el însuși un corp.

(3) PROP. Fie K un corp și fie $k \neq \emptyset$ o submulțime a lui K . Atunci, următoarele afirmații sunt echivalente:

(i) k este un subcorp al lui K ;

(ii) oricare ar fi $x, y \in k$ avem $x-y \in k$, iar dacă $y \neq 0$ atunci $xy^{-1} \in k$.

2. Caracteristica unui corp/inel

Notiunea de caracteristică este consistentă în cazul corpurielor, și nu poate fi definită și pentru un inel unitar. Deci, fie R un inel unitar. Sunt posibile două situații contrare, anume,

- (i) nu există un nr. întreg $n > 0$ s.t. $1+1+\dots+1$ (de n ori) = 0; în acest caz spunem că R are caracteristica zero și scriem $\text{char } R = 0$.
- (ii) În cazul contrar, fie $m > 0$ cel mai mic întreg pt. care $1+\dots+1$ (de m ori) = 0. Acest m există pt. că multimea întregi pozitive este bineordonată. Spunem că inelul R are caracteristica m și scriem $\text{char } R = m$.

(4) EXEMPLU. $\text{char } \mathbb{Z} = 0$. $\text{char } M_m(\mathbb{Z}_6) = 6$.

(5) PROP. Fie R un inel unitar de caracteristică $n > 0$.

- (i) Aplicația $m \mapsto m \cdot 1_R$, $\mathbb{Z} \rightarrow R$ este un morfism unitar cu nucleul $\langle n \rangle = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$.
- (ii) Dacă R este domeniu, atunci n este număr prim.

DEM. (ii) Dacă $n = r \cdot s$, cu $1 < r, s < n$, atunci $0 = n \cdot 1_R = (r \cdot s) \cdot 1_R = r + \dots + r$ (de s ori) $= (\underbrace{1 + \dots + 1}_{\text{de } r \text{ ori}}) \cdot (\underbrace{1 + \dots + 1}_{\text{de } s \text{ ori}}) = (r \cdot 1)(s \cdot 1)$. Din condiție R domeniu rezultă $r \cdot 1_R = 0$ sau $s \cdot 1_R = 0$, contradicție cu ipoteza $\text{char } R = n$. \blacksquare

(6) OBS. Dacă $\text{char } R = n$, atunci $r + \dots + r$ (de n ori) = 0, pt orice $r \in R$.

Pă de altă parte, dacă $r \neq 1$ este posibil ca $r + \dots + r$ (de m ori) = 0, pt $m < n$. De exemplu, pentru $R = \mathbb{Z}_{12}$ avem $\text{char } R = 12$ și totodată $4+4+4=0$, $6+6=0$.

3. Corpuri prime

Sintagma „corpuri prime” nu poate fi înlocuită cu „primele coruri”. Astă cum vom vedea în continuare, primele coruri sunt „prime” la un izomorfism, \mathbb{Q} și \mathbb{Z}_p cu p nr. prim. Aceste coruri nu sunt subcoruri proprii și orice corp conține un alt corp izomorf, fie cu \mathbb{Q} , fie cu un \mathbb{Z}_p .

(7) PROP. Corpurile \mathbb{Q} și \mathbb{Z}_p , cu p număr prim, nu contin subcorpuri proprii și nu sunt izomorfe.

Dem. Fie $k \subseteq \mathbb{Q}$ un subcorp al lui \mathbb{Q} . Atunci $1_{\mathbb{Q}} \in k \Rightarrow m \cdot 1_{\mathbb{Q}} \in k, \forall m \in \mathbb{Z}$. De asemenea, $n \in k \Rightarrow 1_{\mathbb{Q}} \cdot n = n \cdot 1_{\mathbb{Q}}, n \neq 0$. Urmează că $\frac{m}{n} \in k, \forall \frac{m}{n} \in \mathbb{Q}$. Fie $k \subseteq \mathbb{Z}_p$ un subcorp. În particular, k este un subgroup al gr. abelien $(\mathbb{Z}_p, +)$. Din teo. lagrange $\text{ord}(k) \mid \text{ord}(\mathbb{Z}_p) \Rightarrow \text{ord}(k) = p$, deci $\text{ord}(k) > 1$. Dacă $\varphi: \mathbb{Q} \rightarrow \mathbb{Z}_p$ este izomorfism de corpuri, at $\varphi(1_{\mathbb{Q}}) = 1_{\mathbb{Z}_p} \Rightarrow \varphi(p \cdot 1_{\mathbb{Q}}) = p \cdot 1_{\mathbb{Z}_p} = 0$, contradicție cu condiția φ aplicativă injectivă. ■

(8) PROP. Orice corp K conține un subcorp izomorf fie cu \mathbb{Q} , fie cu un corp \mathbb{Z}_p , p prim. Mai precis,

- (i) dacă $\text{char } K = 0$, at. K conține un subcorp izomorf cu \mathbb{Q} ;
- (ii) dacă $\text{char } K = p$, p prim, at. K conține un subcorp izomorf cu \mathbb{Z}_p .

Dem. Fie $j: \mathbb{Z} \rightarrow K$ morfismul unitar de inele $j: m \mapsto m \cdot 1_K$. $\text{Ker } j$ ideal în $\mathbb{Z} \Rightarrow \exists n \geq 0$ s.t. $\text{Ker } j = n\mathbb{Z}$.

(i) Dacă $n = 0$, at. $\text{Ker } j = \langle 0 \rangle$, deci j este un morfism injectiv și j se extinde la un morfism injectiv (unic determinat) $\bar{j}: \mathbb{Q} \rightarrow K$, $\bar{j}\left(\frac{m}{n}\right) = j(m) \cdot (j(n))^{-1}$. Rezulta că imaginea $\bar{j}(\mathbb{Q}) \subseteq K$ este un subcorp izomorf cu \mathbb{Q} .

(ii) Dacă $n > 0$, atunci $\text{char } K = p \Rightarrow n = p$, deci $\text{Ker } j = p\mathbb{Z}$. Imaginea $j(\mathbb{Z})$ a morfismului de grupuri $j: (\mathbb{Z}, +) \rightarrow (K, +)$ cu $\text{Ker } j = p\mathbb{Z}$ este un grup izomorf cu \mathbb{Z}_p . În fine, j se extinde la un morfism injectiv de corpuri $\bar{j}: \mathbb{Z}_p \rightarrow K$. ■

4. Corpul de fractii al unui domeniu

Inelele de fractii ale unui anel comutativ unitar se construiesc după modelul cunoscut al construcției lui \mathbb{Q} din \mathbb{Z} . În general, într-un anel de fractii R_f al anelului R , elementele unei submulțimi $S \subseteq R$ se identifică cu elemente inversibile din R_f .

Legat de scopul nostru ne ocupăm de cazul când anelul de fractii este chiar un corp.

(9) TEOR. Fie R un inel comutativ unitar nenucliar fără divizori ai lui zero și fie $S = R \setminus \{0\}$. Pe mulțimea $R \times S$ definim rel. binară

$$(r,s) \sim (r',s') \text{ dacă } r's = r's'.$$

(i) Relația \sim este o relație de echivalență pe $R \times S$.

(ii) Fie $\frac{r}{s}$ clasa de echivalență a perechii ordonate $(r,s) \in R \times S$ și notăm R_s mulțimea claselor de echivalență. Atunci R_s este un inel comutativ cu adunare și înmulțire definită prin

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'} \quad \text{și} \quad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

(iii) Morfismul $\varphi: R \rightarrow R_s$ dat prin $r \mapsto \frac{r}{1}$ este un morfism injectiv, astfel încât izomorfismul $R \cong \varphi(R) \subseteq R_s$ permite identificarea $r = \frac{r}{1}, \forall r \in R$.

(iv) Elementele $\frac{1}{s}$, $s \neq 0$, sunt inversabile cu inversul $\frac{s}{s}$. Altfel spus, elementele nenele din R sunt inversabile în R_s , via identif. $r = \frac{r}{1}$.

(v) R_s este un corp, numit corpul de fractii al domeniului R . ■

(1.1) DEF. Un corp F este o extindere de coruri (sau pur și simplu extindere) a lui K dacă K este un subcorp al lui F .

Dacă privim pe F ca un sp. vec. peste K , atunci putem vorbi despre dimensiunea $\dim_K F$, pe care văd-o notăm $[F:K]$. Dacă cum dimensiunea $[F:K]$ este finită sau infinită, spunem că F este extindere de dimensiune finită, respectiv extindere de dimensiune infinită. Dimens. $[F:K]$ se mai numește gradul extinderii.

(1.2) PROP. Fie F extindere de coruri a lui E și E extindere de coruri a lui K . Atunci $[F: E] \cdot [E: K] = [F: K]$.

Mai mult, $[F: K]$ este finită $\Leftrightarrow [F: E] \text{ și } [E: K]$ sunt finite.

Dem. Fie U o baza a lui F peste E și V o baza a lui E peste K . Este suficient să arătăm că $\{uv \mid u \in U, v \in V\}$ este o baza a lui F peste K . Pt. acesta observăm că dacă $x \in F$, atunci $x = \sum_{i=1}^m x_i u_i$, unde $x_i \in E$ și $u_i \in U$. Apoi, fiecare x_i se poate scrie $x_i = \sum_{j=1}^n x_{ij} v_j$ ($x_{ij} \in K$, $v_j \in V$). În acest fel

$$x = \sum_{i=1}^m x_i u_i = \sum_{i=1}^m \left(\sum_{j=1}^n x_{ij} v_j \right) u_i = \sum_{i=1}^m \sum_{j=1}^n x_{ij} (u_i v_j),$$

care înseamnă că $\{uv \mid u \in U, v \in V\}$ generază F ca sp. vec. peste K .

Să arătăm că uv , $u \in U, v \in V$ sunt lin. nndep. Pt. acesta,

Fiind $\sum_{i=1}^m \sum_{j=1}^m \alpha_{ij} u_i v_j = 0$, unde $\alpha_{ij} \in K$, $u_i \in U$, $v_j \in V$. Atunci $\sum_{i=1}^m \left(\sum_{j=1}^m \alpha_{ij} v_j \right) u_i = 0$ și cum u_i sunt lin. indep. peste K rezultă că $\sum_{j=1}^m \alpha_{ij} v_j = 0$ pentru toți $i = 1, 2, \dots, n$. În fine, pt. fiecare $i = 1, 2, \dots, n$ avem $\alpha_{ij} = 0$, $j = 1, 2, \dots, m$ deoarece vezi. v_i sunt lin. indep. peste K . Astfel, din $\sum_{i,j} \alpha_{ij} u_i v_j = 0$ rezultă $\alpha_{ij} = 0$ pentru toți indicii i, j , adică $\{uv | u \in U, v \in V\}$ este o mulțime vectorială lin. indep. peste K .

A doua afirmație rezultă din faptul că produsul a două numere cardinale finite este finit, iar produsul unui cardinal infinit cu orice cardinal este infinit. ■

In concl., $K \subset E \subset F$ din Prop. 1.2, se spune că E este un corp intermediar al lui K și F .

Dacă F este un corp și $M \subset F$ o mulțime de elem. din F , atunci subcorful (resp. subinelul) generat de M este intersecția tuturor subcorpuriilor (resp. subinelor) lui F care conțin pe M . Dacă $K \subset F$ este o extindere de corpuri și $M \subset F$, atunci subcorful (resp. subinelul) generat de $K \cup M$ să se numească subcorful (resp. subinelul) generat de M peste K și se notează $K(M)$ (resp. $K[M]$).

Dacă M este mulțime finită, respectiv $M = \{u_1, \dots, u_n\}$, atunci subcorful $K(M)$ (respectiv, subinelul $K[M]$) se notează $K(u_1, u_2, \dots, u_n)$ (resp. $K[u_1, u_2, \dots, u_n]$). Corpul $K(u_1, u_2, \dots, u_n)$ să se numească extindere finită generată a lui K peste K . Dacă $M = \{u\}$, at. $K(u)$ să se numească extindere simplă. Dacă $\sigma \in S_n$, atunci $\{u_{\sigma(1)}, \dots, u_{\sigma(n)}\} = M$,

prin urmare, atât în $K(u_1, \dots, u_n)$ ca și în $K(u_1, \dots, u_n)$ nu depinde ordinea elementelor u_i . De asemenea, $K(u_1, \dots, u_n)(u_n) = K(u_1, \dots, u_n)$ și

$K[u_1, \dots, u_n][u_n] = K[u_1, \dots, u_n]$. Este suficient să arătăm că $K(x)(y) = K(x, y)$:

Așa că $u \in K(x, y) \Rightarrow u \in E$, și E corp ce conține pe $(K \cup \{x\}) \cup \{y\}$

$\Rightarrow u \in E$, și E care conține pe $K(x) \cup \{y\} \Rightarrow u \in K(x)(y)$.

Invers

$x \in K(x)(y) \Rightarrow x \in E$, și E corp care conține pe $K(x) \cup \{y\} \Rightarrow$

$\Rightarrow x \in E$, și E corp care conține pe $K \cup \{x\} \cup \{y\} \Rightarrow$

$\Rightarrow x \in E$, și E care conține pe $K \cup \{x, y\} \Rightarrow$

$\Rightarrow x \in K(x, y)$.

În cele ce urmează, între un corp. elem. uv^{-1} se va nota atesta $\frac{u}{v}$.

(1.3) TEOR. Dacă $K \subseteq F$ este o extindere de corpuri, $u, u_i \in F$ și $M \subset F$, atunci

- Subinelul $K[u] = \{f(u) \mid f \in K[x]\}$
- Subinelul $K[u_1, \dots, u_n] = \{f(u_1, \dots, u_n) \mid f \in K[x_1, x_2, \dots, x_n]\}$
- Subinelul $K[M] = \{h(u_1, \dots, u_n) \mid u_i \in M, m \in \mathbb{N}^* \text{ și } h \in K[x_1, \dots, x_n]\}$
- Subcorpu $K(u) = \{f(u)/g(u) \mid f, g \in K[x] \text{ și } g(u) \neq 0\}$.
- Subcorpu $K(u_1, \dots, u_n) = \{h(u_1, \dots, u_n)/g(u_1, \dots, u_n) \mid h, g \in K[x_1, \dots, x_n], g(u_1, \dots, u_n) \neq 0\}$.
- Subcorpu $K(M) = \{f(u_1, \dots, u_n)/g(u_1, \dots, u_n) \mid m \in \mathbb{N}^*, f, g \in K[x_1, \dots, x_n], g(u_1, \dots, u_n) \neq 0, u_i \in M\}$.

Dem (Schită). (a) Este clar că dacă $K \cup \{u\} \subseteq F$ și $f = a_n X^n + \dots + a_0 \in K[x]$, atunci $f(u) \in K[u]$, deci $\{f(u) \mid f \in K[x]\} \subseteq K[u]$. Pentru incluziunea inversă este suficient să arătăm că $\{f(u) \mid f \in K[x]\}$ este un subinel al lui F care conține pe $K \cup u$, ceea ce este evident deoarece dacă $f, g \in K[x]$, atunci $f - g, fg \in K[x]$.

(f) Orice corp E care conține K și M tb. să contină multimea $E = \{f(u_1, \dots, u_n)/g(u_1, \dots, u_n) \mid m \in \mathbb{N}^*, f, g \in K[x_1, \dots, x_n] \text{ și } g(u_1, \dots, u_n) \neq 0\}$. Pentru incluziunea inversă este suficient să arătăm că E este un corp ce conține pe $K \cup M$.

Fie $f(u_1, \dots, u_n)/g(u_1, \dots, u_n)$ și $f_1(u_1, \dots, u_n)/g_1(u_1, \dots, u_n) \in E$. Atunci, scriind mai scurt avem

$$\begin{aligned} f/g - f_1/g_1 &= fg^{-1} - f_1g_1^{-1} = fg^{-1}g_1g_1^{-1} - f_1g_1g_1^{-1} = fg_1(gg_1)^{-1} - f_1g(gg_1)^{-1} \\ &= (fg_1 - f_1g)(gg_1)^{-1} = \frac{fg_1 - f_1g}{gg_1} \in E \end{aligned}$$

De asemenea,

$$\frac{f}{g} \cdot \frac{f_1}{g_1} = fg^{-1}f_1g_1^{-1} = f_1f_1(gg_1)^{-1} = \frac{f_1f_1}{gg_1} \in E \Rightarrow K(M) \subseteq E. Deci, K(M) = E.$$

Extinderile de corpuri se împart în două clase distincte, în sensul definiției următoare.

(1.4) DEF. Fie $F \supseteq K$ o extindere de câmpuri. Un element $u \in F$ este algebric peste K dacă u este rădăcina unui polinom $f \in K[x]$. Dacă toate elem. $u \in F$ sunt algebrice peste K , atunci se spune că F este o extindere algebrică a lui K . Dacă F nu este o extindere algebrică a lui K , atunci se spune că este o extindere transcendentală a lui K . O extindere este transcendentală dacă cel puțin un element $u \in F$ nu este rădăcintă a vreunui polinom din $K[x]$; un astfel de element s.n. transcendent peste K .

(1.5) EXEMPLU. $i \in \mathbb{C}$ este algebric peste \mathbb{R} , fiind rădăcina polinomului $f = x^2 + 1 \in \mathbb{R}[x]$.

De fapt, $\mathbb{C} = \mathbb{R}(i)$. Numerele $\pi, e \in \mathbb{R}$ sunt transcendente peste \mathbb{Q} , deci $\mathbb{R} \supset \mathbb{Q}$ este extindere transcendentală.

(1.6) EXEMPLU (de extindere transcendentală). Dacă K este un corp, atunci înmulțirea de polinoame $K[x]$ este domeniu. Corpul de fractii al lui $K[x]$, notat $K(x)$, este

$$K(x) = \left\{ \frac{f}{g} \mid f, g \in K[x], g \neq 0 \right\}.$$

$K \subset K(x)$ este extindere de corpuști. Elementul x este transcendent peste K deoarece altfel, ar exista un polinom $h \in K[y]$, $h = a_0 + a_1 y + \dots + a_n y^n$ și $h(x) = 0$, adică $a_0 + a_1 x + \dots + a_n x^n = 0$. Dar ultima relație ar cădea în contradicție cu $(a_0, a_1, \dots) = (0, 0, \dots)$.

In altă ordine de idei, $K(x)$ este un exemplu de extindere finit generată care nu este de dimensiune finită. Pentru acestă să punem pe $K(x)$ ca subcorpul lui $K(x,y)$ generat de $K[x]$ peste K . Multimea $\{1, x, x^2, \dots\}$ este liniar independentă peste K , prin urmare $K(x)$ este extindere de dimensiune infinită peste K .

Mai general, $K(x_1, \dots, x_n)$, corpul de fractii al lui $K[x_1, x_2, \dots, x_n]$, este o extindere transcendentală a lui K , finit generată, dar nu de dimensiune finită.

Următoarele două propoziții caracterizează extinderile simple $K(u)$, după cum u este algebraic sau transcendent.

(1.7) PROP. Fie $K \subseteq F$ o extindere de corpuști. Dacă $u \in F$ este transcendent peste K , atunci există un izomorfism de corpuști $K(u) \cong K(x)$ care este aplicarea identității pe K .

Dem. Deoarece u este transcendent $f(u) \neq 0$ și $g(u) \neq 0$ pt. bți $f, g \in K[x]$. Aplicarea $\varphi: f/g \mapsto f(u)/g(u) = f(u)/g(u)^{-1}$, $\varphi: K(x) \rightarrow K(u)$ este bine definită pe corpul de fractii $K(x)$ al lui $K[x]$ (adică, dacă $f/g = f'/g'$, atunci $\varphi(f/g) = \varphi(f'/g')$). φ este monomorfism și $\varphi|_K = \text{id}_K$. În final, $\text{Im } \varphi = K(u)$, deci $K(u) \cong K(x)$.

(1.8) OBS. Dacă u este transcendent peste K , atunci $xu, a \in K^*$ și puterile $u^n, n \in \mathbb{N}$ sunt elemente transcendente. În schimb, dacă u^n ar fi algebraic și $a_0 + a_1 u^n + \dots + a_k (u^n)^k = 0$, $a_i \in K$ (nu toti nuli), atunci u ar fi radacina a polin. $a_0 + a_1 x^n + \dots + a_k x^{nk} \in K[x]$.

(1.9) TEOR. Fie $K \subseteq F$ o extindere de corpuri. Dacă $u \in F$ este algebric peste K , atunci:

- (a) $K(u) = K[u]$;
- (b) $K(u) \cong K[x]/(f)$, unde $f \in K[x]$ este un polinom monic ireductibil de grad $n \geq 1$, unic determinat de condițiile $f(u)=0$ și $g(u)=0$, $g \in K[x]$ d.s.n.d. f divide g (f este monic deci $\text{lc}(f)=1$).
- (c) $[K(u) : K] = m$;
- (d) $\{1, u, u^2, \dots, u^{m-1}\}$ este o bază a sp.vct. $K(u)$ peste K .
- (e) orice element din $K(u)$ se scrie în mod unic sub forma $a_0 + a_1 u + \dots + a_{m-1} u^{m-1}$ ($a_i \in K$);

Dem: (b) și (a). Considerăm aplicația $\varphi: K[x] \rightarrow K[u]$ dată prin $f \mapsto f(u)$. φ este epimorfism de inele alei, $K[u] \cong K[x]/\text{Ker } \varphi$. Deoarece $K[x]$ este principal, $\exists f \in K[x], f \neq 0, f(u)=0$ a.s. $\text{Ker } \varphi = (f)$. În plus, $(f) \neq K[x]$ deoarece $\text{Ker } \varphi = K[x]$ înseamnă $\varphi = 0$. În fine, $\text{grad}(f) \geq 1$. Deci $\text{lc}(f) = c \neq 1$, deci polinomul $c^{-1}f$ este monic, iar $\langle f \rangle = \langle c^{-1}f \rangle$.

Pentru urmare, putem presupune că f este monic. Deci, $K[u] \cong K[x]/(f)$, f monic nemul si neconstant cu $f(u)=0$. Deoarece $K[x]/(f)$ este domeniul rezultat $\langle f \rangle$ este prim în $K[x]$. Cu Teor. 9 din L7 avem $\langle f \rangle$ prim $\Rightarrow f$ prim $\Rightarrow f$ ireductibil $\Rightarrow \Rightarrow \langle f \rangle$ maximal, deci $K[u]$ este corp. Deoarece $K(u)$ este cel mai mic corp ce conține pe $K \cup \{u\}$ rezultă că $K[u] \supseteq K(u)$. Deci $K[u] = K(u)$. Unicitatea lui f rezultă din faptul că f este monic, iar dacă $g(u)=0$ atunci $g \in \langle f \rangle$ și $f | g$.

(d) Din (a) rezultă că orice element din $K(u) = \{f(u)(g(u))^{-1} \mid h, g \in K[x], g(u) \neq 0\}$ are o reprezentare de forma $p(u)$, unde $p \in K[x]$. Din teorema împ. cu rest., $p = fq + r$, unde $q, r \in K[x]$ și $\text{grad}(r) \leq m-1$. Rezultă că $p(u) = r(u) = a_0 + a_1 u + \dots + a_{m-1} u^{m-1}$, $a_i \in K$. Ac. înseamnă că mulțimea $\{1, u, \dots, u^{m-1}\}$ generă pe $K(u)$. Să arătăm că $\{1, u, \dots, u^{m-1}\}$ este alcătuită din vectori liniari independenți. Pentru acesta, fie

$$a_0 + a_1 u + \dots + a_{m-1} u^{m-1} = 0 \quad (a_i \in K).$$

Atunci $g = a_0 + a_1 X + \dots + a_{m-1} X^{m-1} \in K[X]$ are pe u ca ridicare și $\text{grad}(g) \leq m = \text{grad}(f)$.

Pe de altă parte, $f | g \Rightarrow g = 0$, prin urmare, $a_i = 0$ pentru toți i.

(c) și (e). Sunt consecințe imediate ale punctului (d). ■

(1.10) DEF. Fie $K \subseteq F$ o extindere de corpuri și $u \in F$ algebric peste K . Polinomul f din Teor. 1.9 s.n. polinomul minimul al lui u. Numărul $m = \text{grad}(f) = [K(u) : K]$ s.n. gradul lui u peste K

- (1,II) EXEMPLU. (a) Considerăm extinderea $\mathbb{Q} \subseteq \mathbb{R}$. Elementul $\sqrt{2} \in \mathbb{R}$ este algebric peste \mathbb{Q} , având polinomul minimul $f = x^2 - 2 \in \mathbb{Q}[x]$. Gradul lui $\sqrt{2}$ este 2, iar o bază a corpului $\mathbb{Q}(\sqrt{2})$ este $\{1, \sqrt{2}\}$. Atunci, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
- (b) Fie extinderea $\mathbb{Q} \subseteq \mathbb{R}$ și polinomul $f = x^3 - x + 1 \in \mathbb{Q}[x]$. f este ireductibil peste \mathbb{Q} deoarece singurile posibile rădăcini rationale sunt $1 \text{ și } -1$. Pe de altă parte, f are cel puțin o rădăcină reală, fiindcă $\deg(f)$ este impar. Fie $u \in \mathbb{R}$ a.t. $f(u) = 0$. Atunci, $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ și $\{1, u, u^2\}$ este o bază a lui $\mathbb{Q}(u)$ peste \mathbb{Q} . Toate elementele lui $\mathbb{Q}(u) = \mathbb{Q}[u]$ pot fi scrisă ca o comb. liniară a elementelor bazei. De exemplu, pt. la $x = 3u^5 + 2u^4 + 4u + 4$ să se scrie ca o comb. liniară a lui 1, u și u^2 efectuăm împărțirea în rest a polin. $3x^5 + 2x^4 + 4x + 4$ la $x^3 - x + 1$ și obținem
- $$3x^5 + 2x^4 + 4x + 4 = (x^3 - x + 1)(3x^2 + 2x + 3) + (-x^2 + 5x + 1),$$

de unde

$$\begin{aligned} 3u^5 + 2u^4 + 4u + 4 &= (u^3 - u + 1)(3u^2 + 2u + 3) + (-u^2 + 5u + 1) \\ &= -u^2 + 5u + 1. \end{aligned}$$

Să calculăm inversul elem. $x = -u^2 + 5u + 1$. Polinomul $x^3 - x + 1$ fiind ireductibil, rezultă că $x^3 - x + 1$ și $-x^2 + 5x + 1$ sunt prime între ele. În consecință, $\exists v, w \in \mathbb{Q}[x]$ a.t.

$$(x^3 - x + 1)v(x) + (-x^2 + 5x + 1)w(x) = 1$$

Rezultă că $(-u^2 + 5u + 1)v(u) = 1$. Cu algoritmul lui Euclid s-a obținut

$$v(x) = 25/494x - 131/494 \text{ și } w(x) = -\frac{25}{494}x^2 + \frac{3}{247}x - \frac{640}{247}, \text{ prin urmare}$$

$$(-u^2 + 5u + 1)^{-1} = -\frac{25}{494}u^2 + \frac{3}{247}u - \frac{640}{247}.$$

$$(u+1)^{-1} = ?$$

EXERCITIU. Fie $K \subseteq F$ o extindere de corpuri.

1. (a) $[F : K] = 1 \iff F = K$.
 - (b) Dacă $[F : K]$ este prim, atunci nu există corpuri intermedii între K și F .
 - (c) Dacă $u \in F$ are gradul n peste K , atunci n divide $[F : K]$.
2. Dacă $u_1, \dots, u_m \in F$, atunci corpul $K(u_1, \dots, u_m)$ este (izomorf cu) corpul de fractii al inelului $K[u_1, \dots, u_m]$.
 3. Dacă v este algebric peste $K(u)$, pentru un $u \in F$ și v este transcendent peste K , atunci u este algebric peste $K(v)$.

4. Fie $a \neq 0$ rădinește polinomului $f = x^3 - x + 1 \in \mathbb{Q}[x]$. Se cere să se scrie inversul lui $1 - 2a + 3a^2$ în $\mathbb{Q}(a)$, în funcție de baza $\{1, a, a^2\}$. Care este inversul lui a ?

5. Se cere să se arate că pentru orice nr. natural $n \geq 1$ există în $\mathbb{Q}[x]$ un polinom ireductibil de grad n . În particular, deduci că pentru orice $n \geq 1$ există o extindere finită de grad n a lui \mathbb{Q} .

6. Se cere să se arate că singurile polin. ireductibile din $\mathbb{R}[x]$ sunt polinoame de gradul 1 și cele de gradul 2 de forma $ax^2 + bx + c$ cu $b^2 - 4ac < 0$.

Sol. Folosim proprietatea că orice polinom din $\mathbb{R}[x]$ are cel puțin o rădine (în fiz., toate rădările) în \mathbb{C} , și că $\mathbb{C} = \mathbb{R}[i]$.

7. Dacă $u \in F$ este algebric de grad impar peste K , atunci tot astfel este și u^2 . Mai mult, $K(u) = K(u^2)$. (Ind. Se folosește rel. gradele între extinderi.)

Rădăcini ale polinoamelor

Corpul de descompunere al unui polinom

In această lecție ne vom ocupa, în principal, de polinoamele ireductibile peste un corp K . Vom arăta că pentru orice polinom $f \in K[x]$ există o extindere $K \subseteq F$ în care f se descompune în factori de gradul unu. În acest scop, ne vom folosi în mod constant de noțiunea de rădăcină a unui polinom, pe care o remarcăm împreună cu câteva proprietăți ale sale.

Fie R un inel comutativ nul. Elementul $a \in R$ este rădăcină a polinomului $f \in R[x]$ dacă $f(a) = 0$. De exemplu, $a=1$ este rădăcină a polinomului $f = x^3 - 1 \in R[x]$.

1. PROP. (Teorema Bezout). Fie R un inel comutativ, $f \in R[x]$ și $a \in R$.

- Restul împărțirii lui f la $x-a$ este $f(a)$;
- a este rădăcină a lui $f \Leftrightarrow x-a$ divide pe f .

Dem. Se poate folosi demonstrația teoremei împărțirii cu rest a polinoamelor: $f = (x-a)q + r$, unde $\text{grad}(r) < 1$, deci $r \in R$. Dacă facem $x=a$, atunci $r = f(a)$. ■

2. COROLAR. Fie D un domeniu, $f \in D[x]$ un polinom nul, $a \in D$ și rădăcină a lui f și $n \geq 1$.

$(x-a)^n$ divide pe f și $(x-a)^{n+1}$ nu divide $f \Leftrightarrow f$ se scrie $f = (x-a)^n g$, cu $g \in D[x]$ și $g(a) \neq 0$.

Dem. Rezultă din Teorema Bezout. ■

In condițiile corolarului precedent se spune că a este rădăcină a lui f cu ordinul de multiplicitate n sau rădăcină de ordinul n . De exemplu, $a=-2$ este rădăcină de ordinul 3 a polinomului $f = x^4 + 5x^3 + 6x^2 - 4x - 8$.

3. TEOR. Fie D un domeniu, $0 \neq f \in D[x]$ și $a_1, a_2, \dots, a_s \in D$ rădăcinile distincte ale lui f , respective de ordine n_1, n_2, \dots, n_s . Atunci f se poate scrie sub forma

$$f = (x-a_1)^{n_1} (x-a_2)^{n_2} \cdots (x-a_s)^{n_s} g, \quad (1)$$

unde $g \in D[x]$ și a_1, a_2, \dots, a_s nu sunt rădăcini ale lui g .

Dem (prin inducție după s). Pentru $s=1$ afirmația rezultă din corolarul 2. Pres. afirmația adică $\exists t \in S$ și $\exists g \in D$ astfel încât $f = t g$. Deoarece $t \in S$ și $t \neq 0$, atunci t nu este rădăcină a lui f .

$$f = (x-a_1)^{n_1} \cdots (x-a_{s-1})^{n_{s-1}} f_1,$$

unde a_1, \dots, a_{s-1} nu sunt rădăcini ale lui f_1 . Avem că

$$(x-a_s)^{n_s} \mid f \Rightarrow (x-a_s)^{n_s} \mid (x-a_1)^{n_1} \cdots (x-a_{s-1})^{n_{s-1}} f_1. \text{ Polinom.}$$

$x-a_1, \dots, x-a_s$ sunt prime între ele și $(x-a_1)^{n_1}, \dots, (x-a_s)^{n_s}$ sunt prime între ele și $(x-a_s)^{n_s}$ prim cu $(x-a_1)^{n_1} \cdots (x-a_{s-1})^{n_{s-1}}$.

Rezultă că $(x-a_s)^{n_s} \mid f_1$, făcând ceea ce încheie demonstrația. \square

Rezultă că numărul rădăcinilor unui polinom nu este egal cu numărul rădăcinilor distincte, ci cu suma ordinilor de multiplicitate ale lor. De exemplu, numărul rădăcinilor polinomului

$$X^4 + 5X^3 + 6X^2 - 4X - 8 = (X+2)^3(X-1)$$

este egal cu 4: rădăcinile sunt $-2, -2, -2$ și 1 .

4. COROLAR. Un polinom de gradul $n \geq 1$ cu coeficienți întregi din domeniu D are cel mult n rădăcini în D .

Dem. Rezultă din relație (1).

Ipozită D domeniu din Cor. 4 este evidentă. De exemplu, polinomul $f = X^2 - 4 \in \mathbb{Z}_{12}[X]$ are trei rădăcini în \mathbb{Z}_{12} , numai 2, 4 și 8. Mai mult, polinomul $f = (0,1) \times e(\mathbb{Z} \times \mathbb{Z})[X]$ are ∞ infinitate de rădăcini, numai $(m, 0)$ cu $m \in \mathbb{Z}$.

5. PROP (relație lui Viète). Fie D un domeniu și $f = a_0 + a_1 X + \cdots + a_n X^n \in D[X]$ un polinom de gradul $n \geq 1$. Dacă x_1, x_2, \dots, x_n sunt n rădăcini ale

lui f în D , atunci

$$f = a_n(x-x_1)(x-x_2) \dots (x-x_n),$$

iar în corpul de fractii al lui D are loc relațiile lui Viète:

$$\begin{cases} x_1 + x_2 + \dots + x_n = -a_{n-1}/a_n \\ x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n = a_{n-2}/a_n \\ \dots \\ x_1x_2 \dots x_n = (-1)^n a_0/a_n \end{cases}$$

Dem. Rezultă din identificările ale coeficientilor. ■

6.COR.(Tez. lui Wilson) Dacă p este un nr. prim, atunci $(p-1)! \equiv -1 \pmod{p}$.

Dem. Considerăm polinomul $f = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Deoarece $\text{ord}(\mathbb{Z}_p^*) = p-1$ rezultă că $a^{p-1} = 1, \forall a \in \mathbb{Z}_p^*$. Atât timp, $\hat{1}, \hat{2}, \dots, \hat{p-1}$ sunt $p-1$ radici ale lui f . Ultima relație a lui Viète ne dă

$$\hat{1} \cdot \hat{2} \cdots (\hat{p-1}) = -\hat{1}$$

în \mathbb{Z}_p , respectiv $(p-1)! \equiv -1 \pmod{p}$. ■

7.Teor. Fie K un corp. Dacă $f \in K[X]$ este un polinom ireductibil, atunci există o extindere $K \subseteq F$ în care f are cel puțin o rădăcină.

Mei precis, $F := K[X]/\langle f \rangle$ este o extindere finită a lui K , de grad egal cu $\text{grad}(f)$ și clasa lui X în corpul F este o rădăcină a lui f .

Dem. Deoarece f este ireductibil, idealul $\langle f \rangle = fK[X]$ este maximal în inelul $K[X]$. Atunci $F = K[X]/\langle f \rangle$ este un corp. În F avem $\hat{f} = \hat{0}$. Dacă $f = a_0 + a_1X + \dots + a_nX^n$, $a_n \neq 0$, atunci $\hat{a}_0 + \hat{a}_1\hat{X} + \dots + \hat{a}_n(\hat{X})^n = 0$. Mai departe, scăsură este următoarea.

Notăm $u := \hat{X}$. Aplicația $K \rightarrow F, x \in K \mapsto \hat{x} \in F$ este un morfism injectiv de corpuri \Rightarrow elementele $x \in K$ se identifică cu imaginile lor $\hat{x} \in F$. În consecință, $a_0 + a_1u + \dots + a_nu^n = 0$. Fiind în situație $K \subseteq F$ extindere de corpuri și $u \in F$ element algebraic peste K , în continuare aplicăm Tez. 1.9 din Lecția 5 (9-8/10) ■

8. OBS. Așa cum rezultă din demonstrație Teor.7, u este rădincină
nu chiar și lui $f \in K[x]$, ci și unui polinom din $K'[x]$, unde
 $K' \subseteq F$ este copia izomorfă a lui K . Identificând pe K cu copia
se izomorfă K ($K \cong K' \subseteq F$) din F , spunem că u este rădincină
a lui f în F .

Dacă le monomorfismul $\lambda \mapsto \hat{\lambda}$ de mai
înainte.

9. EXEMPLU. $f = x^2 + 1 \in R[x]$ este ireductibil. $F = R[x]/\langle f \rangle$ este
un corp. în care $(\hat{x})^2 + \hat{1} = \hat{0}$. Notăm $\theta = \hat{x}$. Elementele lui F
se scriu sub forma

$$\hat{a} + \hat{b}\theta, \quad \theta^2 = -1.$$

Apliția

$$i: R \longrightarrow F, \quad r \mapsto \hat{r} = r \pmod{f}$$

fiind morfism injectiv de corperi, identificăm \hat{r} cu $r \in R$. Folosind
relația $R \cong i(R) \subseteq F$, R este perceput ca un subcorp al
lui F . În consecință, elementele lui F se scriu

$$a + b\theta, \text{ unde } a, b \in R \text{ și } \theta^2 = -1$$

θ baza a lui F peste R este $B = \{1, \theta\}$. Adunarea și înmulțirea
din F se efectuează astfel:

$$\begin{aligned} (a+b\theta) + (c+d\theta) &= (a+c) + (b+d)\theta, \\ (a+b\theta) \cdot (c+d\theta) &= ac + ad\theta + bc\theta + bd\theta^2 \\ &= (ac - bd) + (ad + bc)\theta. \end{aligned}$$

θ construcție elementară unui corp în care polinomul
 $f = x^2 + 1 \in R[x]$ nu are rădini și rădina se realizează pe produsul
cartezian $R \times R$ pe care definim

$$(a, b) + (c, d) := (a+c, b+d),$$

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Notăm $C := (R \times R, +, \cdot)$. Elementul 0 în C este parțiala $(0, 0)$,
iar elementul unitate este parțiala ordinată $(1, 0)$. Cu notația
 $i := (0, 1)$ avem rel. exch ($\text{în termeni de parțiale ordonate}$)

$$(0, 1)^2 + (1, 0) = (0, 0),$$

care înseamnă că i este rel. polinomului $(1, 0)x^2 + (1, 0) \in C[x]$.

Apliția

$$\mu: r \mapsto (r, 0), \quad \mu: R \longrightarrow R' = \{(r, 0) \mid r \in R\}$$

fiind izomorfism de corperi, identificarea $r = (n, 0)$ permite

LIV-2
 scrierea polinomului $(1,0)X^2 + (1,0)$ sub forma $X^2 + 1$, prin urmare, $i \in \mathbb{C}$ este ~~ridicătoare~~ ^{considerat} polinomul înțit $f = X^2 + 1 \in \mathbb{R}[x]$.

10. EXEMPLU. $K = \mathbb{Q}$ și $f = X^2 + 1 \in \mathbb{Q}[x]$. O extindere $\mathbb{Q} \subseteq F$ în care f are o radicantă este $\mathbb{Q}(i) = \mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$.

11. EXEMPLU. $f = X^2 - 3 \in \mathbb{Q}[x]$ este un polynom ireductibil. O extindere $\mathbb{Q} \subseteq F$ în care f are o radicantă este $\mathbb{Q}(\sqrt{3})$.

Referitor la domeniile extinderi în care un polynom ireductibil are o radicantă, așe căcum sunt $\mathbb{R}(\theta) \cong \mathbb{C}$ din Exemplul 9 avem următoarele corectitudini.

12. PROP. Fie K un corp și $f \in K[x]$ un polynom ireductibil. Dacă $K \subseteq F$ și $K \subseteq F'$ sunt domenii extinderi ale lui K în care f are radici $\theta \in F$, respectiv $\theta' \in F'$, atunci $K(\theta) \cong K(\theta')$ sunt K -izomorfe printr-un izomorfism care ducă θ în θ' .

Dem. Putem presupune f monic. Deoarece $\theta \in F$ este rad. f , at. θ este algebraic peste K , deci $K(\theta) \cong K[x]/\langle f \rangle$. Analog, $K(\theta') \cong K[x]/f$. Acele izomorfisme sunt K -morfisme care duc pe x în θ , respectiv x în θ' . Cu transițivitatea rel. de izom., $K(\theta) \cong K(\theta')$ printr-un K -izom. care ducă θ în θ' . ■

13. PROP. Dacă K este un corp, atunci pentru orice polynom $f \in K[x]$ de grad $f = n \geq 1$ există o extindere finită în care f are n radici.

Dem. Prin inducție după n . Exercițiu ■

14. DEF. Fie K un corp și fie $K \subseteq F$ o extindere în care polinomul $f \in K[x]$ de gradul n are radici $\theta_1, \theta_2, \dots, \theta_n$. Atunci $K(\theta_1, \theta_2, \dots, \theta_n)$ s.n. corp de descompunere sau de reducibilitate a lui f .

Observații

I f ireductibil peste $K \Rightarrow f$ nu are răd. în K , deci nu și inversa f este irreductibil peste K .

De ex.,

$f = x^4 + 1 \in \mathbb{R}[x]$ nu are răd. în \mathbb{R} , deci este reductibil peste \mathbb{R} :

$$f = x^4 + 1 + 2x^2 - 2x^2 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

Pe de altă parte,

$$f = x^4 + 1 \in \mathbb{Q}[x] \text{ este irred. / } \mathbb{Q}.$$

II $f = x^2 + x + 1 \in \mathbb{R}[x]$ este irred. peste \mathbb{R} .

Fie Θ o răd. într-o extindere, de ex. $F = \mathbb{R}[x]/\langle f \rangle$.

Oricine $x \in F$ este de forma $x = a + b\Theta$, $a, b \in \mathbb{R}$ și $\Theta^2 + \Theta + 1 = 0$. $F = \mathbb{R}(\Theta)$, înmulțirea se face după regula

$$(a+b\Theta)(c+d\Theta) = ac - bd + (ad + bc - bd)\Theta.$$

Pe de altă parte, f are răd. în \mathbb{C} . Dacă $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, atunci $\bar{\varepsilon}$ este cealaltă rădăcină. $F = \mathbb{R}(\varepsilon)$ este o extindere în care ε este o răd.

$$\mathbb{R}(\Theta) \cong \mathbb{R}(\varepsilon)$$

$\mathbb{R}(\varepsilon) = \mathbb{R}(i) = \mathbb{C}$ deoarece $\varepsilon \in \mathbb{R}(i) \Rightarrow \mathbb{R}(\varepsilon) \subseteq \mathbb{R}(i)$ și, invers, $\mathbb{R}(i) \subseteq \mathbb{R}(\varepsilon)$

deoarece $\frac{1}{2} \in \mathbb{R}$ și $\varepsilon + \frac{1}{2} \in \mathbb{R}(\varepsilon) \Rightarrow i\frac{\sqrt{3}}{2} \in \mathbb{R}(\varepsilon) \Rightarrow \frac{2}{\sqrt{3}}(i\frac{\sqrt{3}}{2}) \in \mathbb{R}(\varepsilon)$, nsp. $i \in \mathbb{R}(\varepsilon)$.

III Fix $f = (x^2 - 3)(x^2 - 1) \in \mathbb{Q}[x]$. f are răd. în extinderea $\mathbb{Q}(\sqrt{3}, i)$.

Elem. lui $\mathbb{Q}(\sqrt{3}, i)$ sunt de forma $g(\sqrt{3}, i)$, unde $g \in \mathbb{Q}[x, y]$ și

$$(\sqrt{3})^2 = 3, i^2 = -1, \text{ și } g(\sqrt{3}, i) = g(\sqrt{3}, i), \text{ ad. } x = a + b\sqrt{3} + ci + di\sqrt{3}.$$

În fine

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Corpul de descompunere al unui polinom (contin)

In lecția precedente sună definit notiunea de corp de descompunere al unui polinom. Semnificația noastră este aceea că, dacă $f \in K[x]$, unde K este un corp, este un polinom de gradul n și $\theta_1, \theta_2, \dots, \theta_n$ sunt rădăcinile lui f într-o extindere $F \supseteq K$ a lui K , atunci f văzut ca un polinom cu coeficienți în $K(\theta_1, \theta_2, \dots, \theta_n)$ se descompune în factori liniari, de forma

$$f = c(x - \theta_1)(x - \theta_2) \dots (x - \theta_n), \quad c \in K(\theta_1, \dots, \theta_n). \quad (1)$$

Rădăcinile $\theta_1, \theta_2, \dots, \theta_n$ nu sunt neapărat distincte. Corpul $K(\theta_1, \theta_2, \dots, \theta_n)$ sună corp de descompunere al lui f tocmai pt. că este cel mai mic subcorp al lui F în care f are descompunerea (1).

Corpul de descompunere al polinomului f depinde atât de K cât și de f . Astfel, dacă $f = x^2 + 1 \in \mathbb{Q}[x]$, atunci în extinderea $\mathbb{C} \supseteq \mathbb{Q}$ corpul de descompunere al lui f este $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$. Însă, dacă $f = x^2 + 1 \in \mathbb{R}[x]$, atunci în extinderea $\mathbb{C} \supseteq \mathbb{R}$ corpul de descompunere al lui f este chiar \mathbb{C} deoarece $\mathbb{C} = \mathbb{R}(i)$.

Din Prop. 12 (L10-5) reținem că dacă $f \in K[x]$ este ireductibil și θ, θ' sunt rădăcinile lui f în două extinderi $F \supseteq K$, respectiv $F' \supseteq K$, atunci $K(\theta) \cong K(\theta')$ printr-un K -izomorfism care duce pe θ în θ' . Teorema care urmărește ne arăză că dacă $\theta_1, \dots, \theta_n$ sunt rădăcinile lui f în F , iar $\theta'_1, \dots, \theta'_n$ sunt rădăcinile lui f în F' , atunci $K(\theta_1, \dots, \theta_n) \cong K(\theta'_1, \dots, \theta'_n)$ printr-un K -izomorfism. În termeni de structuri algebrice, pt. faptul că oricare două corpuși de descompunere sunt K -izomorfe se spune că corpul de descompunere al unui polinom este unic, printr-un izomorfism.

TEOR. 1. Două corpuși de descompunere ale unui polinom cu coeficienți într-un corp K sunt K -izomorfe. Mai precis, dacă $f \in K[x]$ este un polinom de gradul n , și $\theta_1, \theta_2, \dots, \theta_n$ sunt rădăcinile lui f în extinderea $F \supseteq K$, iar $\theta'_1, \theta'_2, \dots, \theta'_n$ sunt rădăcinile lui f în extinderea $F' \supseteq K$, atunci corpușile $K(\theta_1, \dots, \theta_n)$ și $K(\theta'_1, \dots, \theta'_n)$ sunt K -izomorfe.

Dem. (inductie după $n = \text{grad } f$). Dacă $\text{grad } f = 1$, atunci $\theta_1 = \theta'_1 \in K$, deci $K(\theta_1) = K = K(\theta'_1)$.

Pres. că proprietatea este adevarată pentru toate polinoamele de grad $< m$ și că
 $f \in K[x]$ cu $\text{grad}(f) = n$. Pres. că $f = pg$, p ireductibil în $K[x]$. Fie θ_1
& rădăcina a lui p în F și fie θ'_1 & rădăcina a lui p în extinderea F' .
Din Prop. 12, $\exists u: K(\theta) \xrightarrow{\sim} K(\theta'_1)$ un K -izomorfism cu $u(\theta) = \theta'_1$. Notăm $L = K(\theta)$
& $L' = K(\theta'_1)$. În $L[x]$ f se scrie $f = (X - \theta_1)f_1$, iar în $L'[x]$ f se scrie $f = (X - \theta'_1)f'_1$,
unde $f_1 \in L[x] = K(\theta)[x]$, $f'_1 \in L'[x] = K(\theta'_1)[x]$. E clar că $f'_1 = u(f_1)$ este poli-
nomul obținut din f_1 înlocuind pe θ_1 cu θ'_1 . Considerăm $v: L[x] \rightarrow L'[x]$
izomorfismul care extinde pe u punând $v(X) = X$. Evident $F \& F'$ sunt
extinderi ale lui L , respectiv L' în care f_1 și f'_1 sunt corpori de descompunere.
Din ipoteza de inducție, $f_1 = c_1(X - \theta_2) \dots (X - \theta_m)$ și $f'_1 = c'_1(X - \theta'_2) \dots (X - \theta'_m)$
unde $c_i \in L(\theta_2, \dots, \theta_m)$ și $c'_i \in L'(\theta'_2, \dots, \theta'_m)$. Din ipot. de inducție, există un
izomorfism $w: L(\theta_2, \dots, \theta_m) \rightarrow L'(\theta'_2, \dots, \theta'_m)$ care extinde pe v și, implicit
extinde și pe u . ■

2. COR. Dacă corpori finiti cu același nr. de elemente sunt izomorfe.

Dem. Fie K un corp finit cu n elemente. Atunci, grupul multiplicativ (K^*, \cdot) are ordinalul $n-1$. În consecință, oricare $x \in K^*$ verifică relația
 $x^{n-1} = 1$. Rezultă că corpul K este un corp de descompunere al polinomului
 $X^n - X \in P[x]$, unde P este corpul prim continețut în K . ■

3. APLICAȚIE. Sa găsim un corp de descompunere al polinomului $X^4 + 1 \in \mathbb{Z}_3[x]$.

Sol. Polinom $f = X^4 + 1 \in \mathbb{Z}_3[x]$ nu are rădăcini în \mathbb{Z}_3 . Dacă este ireductibil,
atunci se descompune într-un produs de două polinoame de gradul al
dilea, anume

$$X^4 + 1 = (X^2 + aX + 1)(X^2 + bX + 1)$$

sau

$$X^4 + 1 = (X^2 + aX - 1)(X^2 + bX - 1).$$

Se găsește că

$$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$$

și este clar că cele doi factori ai descompunerii sunt polin. ireductibile decare
nu au rădăcini în \mathbb{Z}_3 . Considerăm extinderea lui \mathbb{Z}_3 ,

$$F := \mathbb{Z}_3[x]/\langle X^2 + X + 1 \rangle$$

Cu Teor. 9 (L9) elem. lui F se scriu sub forma $a+bu$, unde $a, b \in \mathbb{Z}_3$, iar u este clasa lui X în F . Elementul $u \in F$ fiind rădincă a lui $X^2 + X - 1$ înseamnă că $X^2 + X - 1$ se descompune în factori liniari. Efectuăm împărțirea

$$\begin{array}{r} X^2 + X - 1 \\ -X^2 - ux \\ \hline (1+u)x - 1 \\ -(1+u)x - u^2 - u \\ \hline u^2 + u - 1 \end{array} \quad \begin{array}{l} \text{se obține descompunerea} \\ X^2 + X - 1 = (X-u)(X+1+u) \end{array}$$

În continuare, trebuie să găsim un corp în care polinomul $X^2 + X - 1 \in F[x]$ să aibă rădini. Sunt două variante:

a) polinomul are o rădincă în F ;

b) continuăm extinderea identificând o rădincă în corpul $F[x]/\langle X^2 + X - 1 \rangle$.

$X^2 + X - 1$ are o rădincă în F dacă și există $a, b \in \mathbb{Z}_3$ și astfel $(a+bu)^2 - (a+bu) - 1 = 0$, respectiv

$b(2a-b-1)u + a^2 - 2b^2 - 1 - a = 0$. Elemt. 1, $u \in F$ fiind liniar îndep. peste \mathbb{Z}_3 rezultă sistemul de ec. în \mathbb{Z}_3 :

$$b(2a-b-1) = 0 \Rightarrow a^2 - 2b^2 - a = 1.$$

Sistemul are două soluții, anume $(a, b) = (1, 1)$ și $(a, b) = (0, -1)$, care înseamnă că polinomul $X^2 + X - 1$ are rădăcinile $1+u$ și $-u \in F$. În definitiv, corpul de descompunere al polinomului $X^4 + 1 \in \mathbb{Z}_3[x]$ este $\mathbb{Z}_3(u)$, unde $u = \bar{X}$ în $\mathbb{Z}_3[x]/\langle X^2 + X - 1 \rangle$.

Să avem descompunerea în factori liniari

$$X^4 + 1 = (X-u)(X+1+u)(X-1-u)(X+u) \in F[x].$$

Corpori algebraic închisi

Teorema fundamentală a algebrei

Fie $K \subseteq F$ o extindere de corpori. Se spune că corpul K este algebraic închis în F dacă orice element din F care este algebraic peste K aparține lui K .

Vom spune că un corp K este algebraic închis dacă el este algebraic închis în orice extindere $F \supseteq K$; altfel spus, orice element dintr-o extindere a lui K , care este algebraic peste K , aparține lui K .

4. PROP. Fie K un corp. Următoarele afirmații sunt echivalente:

- (a) K este algebraic închis;
- (b) orice polinom de grad ≥ 1 din $K[x]$ are o rădincă în K ;
- (c) orice polinom de grad ≥ 1 din $K[x]$ are toate rădăcinile în K ;
- (d) orice polinom de grad ≥ 1 din $K[x]$ se descompune în produs finit de factori liniari;

(e) Singurele polinoame ireductibile din $K[x]$ sunt cele de gradul 1.

Dem (a) \Rightarrow (b). Fie $f \in K[x]$, cu $\text{grad}(f) \geq 1$. Există o extindere F a lui K în care f are o răd. x_0 (de ex., $F = K[x]/\langle f \rangle$). Cu ipoteza (a) rezultă că $x_0 \in K$.

(b) \Rightarrow (e). Fie $f \in K[x]$ un polinom ireductibil. Atunci f are o rădincă $x_0 \in K$. Deoarece $\text{grad}(f) > 1$, atunci precum f este ireductibil.

(e) \Rightarrow (d) \Rightarrow (c) \Rightarrow (b) sunt imediate, astfel că avem echivalențele (b) \Leftrightarrow (c) \Leftrightarrow (d) \Leftrightarrow (e). Deci arătăm că (e) \Rightarrow (a), stănci dem. se încheie. Pentru aceasta, fie x_0 un element algebric dintr-o extindere $F \supseteq K$. Multimea $\{f \in K[x] \mid f(x_0) = 0\} =: I$ este un ideal în inelul principal $K[x] \Rightarrow I = \langle p \rangle$, $p \in I$, p ireductibil. Deoarece primul coef. dominant al lui p nu este 1, at. p este unic și s.m. polinomul minimal al lui x_0 . Cu ipoteza (e) rezultă că $\text{grad}(p) = 1$ și, în consecință, $x_0 \in K$. ■

Corpurile \mathbb{Q} și \mathbb{R} nu sunt algebric închise deoarece polinoamile $f = X^2 + 1 \in \mathbb{Q}[x]$, respectiv $f = X^2 + 1 \in \mathbb{R}[x]$ sunt ireductibile. O clasă de corpuri ce nu sunt algebric închise este dată de propoz. următoare.

(5) PROP. Un corp finit nu este algebric închis.

Dem. Fie K un corp finit cu n elemente a_1, a_2, \dots, a_n . Este suficient să arătăm că există un polinom $f \in K[x]$ care nu are nici o rădincă în K . Un astfel de polinom este

$$f = (X - a_1)(X - a_2) \dots (X - a_n) + 1,$$

pentru care $f(x_0) = 1$, $\forall x_0 \in K$. ■

Cel mai important exemplu de corp algebric închis este dat de teorema următoare, cunoscută sub numele de teorema fundamentală a algebrei sau teorema lui d'Alembert pentru care se cunosc aproape 100 de demonstrații. Dem. je care să propunem este preluată din [].

(5) TEOR. Corpul \mathbb{C} al numerelor complexe este algebric închis.

Dem. Se realiză în mai multe etape.

c.) Dacă $f \in \mathbb{R}[x]$ are gradul impar, at. f are o răd. reală. Într-adevăr, notăm

tot ca f să fie polinomul asociat lui f , de la \mathbb{R} la \mathbb{R} . f continuă pe \mathbb{R} , $\lim_{x \rightarrow +\infty} f(x) = \pm \infty$ și $\lim_{x \rightarrow -\infty} f(x) = \mp \infty \Rightarrow \exists R > 0$ a.s. $f(r) \cdot f(-r) < 0$. Prin urmare $\exists a \in \mathbb{R}$ a.s. $f(a) = 0$.

e.) Orice polinom de gradul 2, $f = x^2 + bx + c \in \mathbb{C}[x]$, are 2 rădăcini complexe.

Intr-adevăr, din relație

$$x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4}$$

problema existenței răd. complexe se reduce la existența unei rădăcini reale polinomului $x^2 - \alpha$. Aceasta este o rădăcină de ordinul 2 a nr. complex α .

e.) Orice polinom $f \in \mathbb{R}[x]$ de grad ≥ 2 are 2 rădăcini complexe. Pentru această, f.e. $f \in \mathbb{R}[x]$ și fie $s \in \mathbb{N}$ cel mai mare exponent al lui f pt. care $2^s \mid \text{grad}(f)$. Vom face o dem. prin inducție după s . Deoarece $s=0$, atunci f este impar și afirmația e fort probabilă la f). Pres. afirm. căd. pt. $s-1$ și să o dem. pt.

s. Fie $K = \mathbb{C}(t_1, t_2, \dots, t_n)$ un corp de descompunere al lui f de gradul n peste \mathbb{C} , unde t_1, t_2, \dots, t_n sunt răd. reale. Fie $a \in \mathbb{R}$ și punem

$$u_{ij}^a := a(t_i + t_j) + t_i t_j, \quad 1 \leq i, j \leq n.$$

Considerăm polinomul

$$g_a = \prod_{1 \leq i < j \leq n} (X - u_{ij}^a).$$

$g_a \in K[x]$ și $\text{grad}(g_a) = C_m^2 = \frac{n(n+1)}{2} =: m$. Se observă $2^{s-1} \mid m$, dar $2^s \nmid m$. Coef. polinomului g_a sunt polinome simetrice de u_{ij}^a . Mai mult, ei sunt polinome simetrice în t_1, t_2, \dots, t_n deoarece la o permutare a lor se obține o permutare a elem. u_{ij}^a , deci coeficienți - polinoame număr invariante. Cf. teorema fundam. a polin. simetrice, acesti coef. sunt polinome de s_1, s_2, \dots, s_n , unde

și este polinomul simetric fundamental în t_1, t_n . La rândul lor, s_1, \dots, s_n se scriu cu ajutorul coef. polin. $f \in \mathbb{R}[x]$, prin urmare, $g_a \in \mathbb{R}[x]$. Cf. ipoteza de inducție, g_a are cel puțin 2 răd. complexe, $\forall a \in \mathbb{R}$. Nr. parțialor (i, j) cu $i < j$ este egal cu C_m^2 , pe lângă mult. nr. $a \in \mathbb{R}$ este infinit. At. există doar nr. reale $a \neq b$ a.i. $u_{ij}^a \neq u_{ij}^b$ și fie complexe. Rezulta că diferența $u_{ij}^a - u_{ij}^b = (a-b)(t_i + t_j) \in \mathbb{C}$, respectiv $t_i + t_j \in \mathbb{C}$. De aici, obținem că $t_i + t_j \in \mathbb{C}$.

Așadar, $t_i + t_j$ sunt răd. ale polin.

$$X^2 - (t_i + t_j)X + t_i t_j \in \mathbb{C}[x],$$

deci $t_i + t_j \in \mathbb{C}$.

Varianta. Din definitia polinomului g_a observăm că văzându-l sub forma

$$g_a = g_a(X; u_{12}, u_{13}, \dots, u_{m-1, m}),$$

la anumiteaza $a \in \mathbb{R}[x]$.

orice permutare $\sigma \in S_n$ a indicilor $1, 2, \dots, n$ hădăjește ga neschimbări. Atunci, văzându-l pe ga ca un polinom

$$ga = g_a(X, t_1, t_2, \dots, t_n)$$

observăm că este simetric în t_1, t_2, \dots, t_n . Cu teor. fundam. a polinoamele simetrice rezultă că există un polinom $ha \in \mathbb{R}[x]$: $g_a = ha(X, s_1, s_2, \dots, s_n)$, unde $s_1 = t_1 + \dots + t_n$, $s_2 = t_1 t_2 + t_1 t_3 + \dots + t_n t_n$ etc. Înă, cum s_i se exprimă în funcție de coef. polin. $f \in \mathbb{R}[x]$ rezultă că $g_a \in \mathbb{R}[x]$.

e4) Acum, fie $f = \sum_{i=0}^n a_i x^i \in \mathbb{C}[x]$ un polinom de grad > 1 și fie $\bar{f} = \sum_{i=0}^n \bar{a}_i x^i$, unde \bar{a}_i este conjugatul nr. complex a_i , $i = 0, 1, \dots, n$. Polinomul $f\bar{f}$ este un polinom cu coef. reali devansă $f\bar{f} = \bar{f}f = ff$. Conform l3) ff are cel puțin o rădăcină complexă z_0 . Dacă $f(z_0) \cdot \bar{f}(z_0) = 0$ rezultă că $f(z_0) = 0$ sau $\bar{f}(z_0) = 0$. În cel de-al doilea caz, $\bar{f}(z_0) = 0 \Rightarrow \overline{f(z_0)} = 0$, respectiv $f(\bar{z}_0) = 0$. În definitiv, z_0 sau \bar{z}_0 este o răd. a lui f . ■

6. ADDENDUM. Singurele polinoame ireductibile din $\mathbb{R}[x]$ sunt polinoamele de grad 1 și cele de grad 2 de forma ax^2+bx+c , cu $b^2-4ac < 0$.

Dem. Fie $f \in \mathbb{R}[x]$ un polinom ireductibil de grad > 1 . Atunci f nu are rădăcini reale. Fie $z_0 \in \mathbb{C}$, $f(z_0) = 0$. Atunci, $\overline{f(z_0)} = 0 \Rightarrow f(\bar{z}_0) = 0$, astfel că \bar{z}_0 este și el o rădăcină a lui f. Deci, în \mathbb{C} polinomul f se divide prin $(x-z_0)(x-\bar{z}_0)$, care este un polinom de gradul 2 cu coeficienți reali. Trebuie că $\text{grad}(f) = 2$, pt. că altfel f ar fi ireductibil în $\mathbb{R}[x]$. Astăndată, $f = ax^2+bx+c$, cu $b^2-4ac < 0$.

Teoria lui Galois

1. Definiții de bază

In lecțiile precedente am arătat că pentru orice polinom cu coef. în corpul K există o extindere de corpuri $K \subseteq F$ care să conțină toate rădăcinile polinomului. Mai presus, dacă $f \in K[x]$ are grad $\deg(f) = n$, atunci există un corp $F \supseteq K$ în care f are n rădăcini. Dacă $\theta_1, \dots, \theta_n$ sunt n rădăcini în F , atunci corpul de descompunere $K(\theta_1, \dots, \theta_n)$ este o extindere finită a lui K . Evariste Galois (1811-1832) a intuit legătura înținsă dintre corpul de descomp. $F = K(\theta_1, \dots, \theta_n)$ și un subgrup al grupului $\text{Aut}(F)$, acesta din urmă, la rândul său izomorf cu un grup de permutări. În acest fel, cercetând structura grupului obținem informații despre corpul F , reciproc, din analiza structurii de corp obținem inform. despre grupul $\text{Aut}(F)$; în definitiv, studiul în tandem al grupului și corpului furnizează informații despre ambele结构uri.

1. DEF. Fie $K \subseteq F$ o extindere de corpuri.

- (a) Un izomorfism $\sigma: F \rightarrow F$ s.n. automorfism al lui F . Multimea autom. lui F se notează $\text{Aut}(F)$. Dacă $x \in F$, atunci adesea scriem σx în loc de $\sigma(x)$.
- (b) Se spune că autom. $\sigma \in \text{Aut}(F)$ fixează elem. $x \in F$ dacă $\sigma(x) = x$. Se spune că $\sigma \in \text{Aut}(F)$ fixează multimea $E \subseteq F$ dacă σ fixează fiecare element al multimei E .
- (c) Notăm cu $\text{Aut}_K(F)$ sau $\text{Aut}(F/K)$ multimea tuturor automorfismelor lui F care fixează pe K .

Pentru orice corp F , corpul său prim P este fixat de automorfismele lui F . Într-oarece, corpul prim al lui F este generat de $1 \in F$ și pt. orice $\sigma \in \text{Aut}(F)$, $\sigma: 0 \mapsto 0$ și $\sigma: 1 \mapsto 1$. Atunci $\sigma a = a$, $\forall a \in P$. În particular, corpurile \mathbb{Q} și \mathbb{Z}_p , p prim, au c.p.c. ident. unicul automorfism $\text{Aut}(\mathbb{Q}) = \{1_{\mathbb{Q}}\}$ și $\text{Aut}(\mathbb{Z}_p) = \{1_{\mathbb{Z}_p}\}$.

2. PROP. Pentru orice extindere de corpuri $K \subseteq F$, $\text{Aut}(F)$ este grup împreună cu oper. de compunere a funcțiilor, iar $\text{Aut}_K(F) \subseteq \text{Aut}(F)$ este un subgrup.

Dem. Exercițiu. ■

Următoarea propoziție este principalul instrument în determinarea aut.omorfismelor extinderilor algebrice.

3. PROP. Fie $K \subseteq F$ extindere de corpuri și fie $x \in F$ algebric peste K . At. pt orice $\sigma \in \text{Aut}_K(F)$, σx este x răd. a polinomului minimal al lui x peste K . Asadar, grupul $\text{Aut}_K(F)$ permute rădăcinile polin. ireductibile. Mai general, orice polinom din $K[x]$ ce are pe x ca rădăcină, are de asemenea, pe σx ca rădăcină.

Dem. Pres. că x e răd. a polin. $f = a_0 + a_1 X + \dots + a_n X^n$, $a_i \in K$. At. $a_0 + a_1 x + \dots + a_n x^n = 0$; aplicația σ rel. precedente se obține $0 = \sigma(f) = \sum_{k=0}^n a_k \sigma(x^k) = \sum_{k=0}^n a_k (\sigma(x))^k$, adică $\sigma(x)$ răd. f. ■



4. EXEMPLE

(a) Fie extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$. Dacă $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$, at $\sigma(\sqrt{2}) = \pm \sqrt{2}$, decarece polinomul minimal al lui $\sqrt{2}$ este $X^2 - 2$. Rezultă că

$$\sigma(a+b\sqrt{2}) = a \pm b\sqrt{2}, \text{ oricare } a, b \in \mathbb{Q}.$$

In definiție, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{\tau_{\mathbb{Q}(\sqrt{2})}, \gamma\}$, unde $\tau_{\mathbb{Q}(\sqrt{2})}(a+b\sqrt{2}) = a-b\sqrt{2}$. Pt. că $\gamma^2 = 1$ observăm că $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \langle \gamma \rangle$ este grup ciclic de ordinul 2 generat de γ .

(b) Fie extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$. $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ este complet determinat de acțiunea sa pe $\sqrt[3]{2}$ decarece

$$\sigma(a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2) = a+b\sigma(\sqrt[3]{2})+c(\sigma(\sqrt[3]{2}))^2$$

Pt. că $\sigma(\sqrt[3]{2})$ trebuie să fie x răd. în $\mathbb{Q}(\sqrt[3]{2})$ a polin. $X^3 - 2$ și singura răd. din corp este $\sqrt[3]{2}$ rezultă că $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$.

Acum, schimbăm puțin punctul de vedere. Astfel, în raport cu incluziunea $K \subseteq F$ sălă privim pe K ca un subcorp al lui F

a factorului $x - c$

- * Indiferent de polinomul ce are pe x rad., $\sigma(x)$ este o rad. (numar) a polin. minimial al lui x :
fie $f = f_1 \cdots f_k$, f_i rad. Presupusă că f_i rad. f_j . At. $\sigma(x) \mid i$ și $f \Rightarrow f_1(\sigma(x)) \cdots f_k(\sigma(x)) \neq 0$.
Dacă $\sigma(x)$ rad. f_j , $j \neq i$, atunci din $f_j(\sigma(x)) = 0$ rezultă $\sigma(f_j(x)) = 0$, resp. $f_j(x) = 0$,
contrad. Prin urmare, $\sigma(x)$ este rad. tot a lui f .

în loc să il vedem pe F ca un subcorp al lui K . În ac. vizinătate, observăm că subcorpul K al lui F îl să-ă asocieze un subgrup (anume $\text{Aut}_K(F)$) al grupului $\text{Aut}(F)$. Asocierea subcorp \mapsto subgrup e reciprocă: fie că unui subgrup al lui $\text{Aut}(F)$ i se asociază un subcorp al lui F , cele două propoz. care urmăresc fixează cadrul exact al celor două corespondențe.

PROP.4. Fie F un corp și fie $H \subseteq \text{Aut}(F)$ un subgrup al grupului automorfismelor lui F . Multimea K a elementelor lui F fixate de toate elementele lui H este un subcorp al lui F .

Dem. Fixezi $x, y \in K$ și $\sigma \in H$. Atunci, $\sigma(x) = x$, $\sigma(y) = y$. Avem $\sigma(x+y) = \sigma(x) + \sigma(y) = x+y$ și $\sigma(xy) = \sigma(x)\sigma(y) = xy$, iar $\sigma(x^{-1}) = (\sigma(x))^{-1} = x^{-1}$. Așadar, K subcorp.

Subcorpul $K \subseteq F$ din propoz. precedente s.m. corpus fixat de subgrupul H . Subliniem că p.d. condiția mai slaba $\sigma(E) = E$, $\forall \sigma \in H$ este posibil ca E să fie un corp intermediar $K \subseteq E \subseteq F$ s.t. $\sigma(E) = \{\sigma x \mid x \in E\} = E$.

PROP.5. Asociările subcorp \mapsto subgrup și subgrup \mapsto subcorp, definite mai înainte, inverseză inclusiunea. Mai exact,

- (a) dacă $K_1 \subseteq K_2 \subseteq F$ sunt două subcorpuri ale lui F , atunci $\text{Aut}_{K_1}(F) \subseteq \text{Aut}_{K_2}(F)$;
- (b) dacă $H_1, H_2 \subseteq \text{Aut}(F)$ sunt două subgrupuri cu câmpurile fixate F_1 , respectiv F_2 , atunci $F_1 \subseteq F_2$.

Dem. Exercițiu. ■

6. EXEMPLE. Revenim la Exemplul 4. Tinând cont că \mathbb{Q} e prim avem:

- (a) Dacă $F = \mathbb{Q}(\sqrt{2})$, at. corpul fixat de $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \langle \tau \rangle$ este multimea de elem. din $\mathbb{Q}(\sqrt{2})$ pt. care

$$\tau(a+b\sqrt{2}) = a+b\sqrt{2},$$

căci $a-b\sqrt{2} = a+b\sqrt{2}$. Se obține $K = \mathbb{Q}$.

- (b) În cazul $\mathbb{Q}(\sqrt[3]{2})$ sit. este clar că avem $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \langle 1 \rangle$.

Cele două exemple evidențiază următoarele fapte:

- (a) subcorpul $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ îl asociază subgrupul $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \equiv \text{Aut}(\mathbb{Q}(\sqrt{2}))$ care implica ambele redunțe ale polin. minimul $x^2 - 2$.

(b) în cazul corpului $\mathbb{Q}(\sqrt[3]{2})$, unicul automorfism al lui $\mathbb{Q}(\sqrt[3]{2})$ care fixează elem. lui \mathbb{Q} este $\sigma: \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$, deși polinomul minim $X^3 - 2$ are trei rădăcini.

O explicație pentru ac. situație poate fi legată de următ. descriere între cele 2 extinderi. Astfel, deoarece $\mathbb{Q}(\sqrt[3]{2})$ este corpul de descompunere al polinomului $f = X^3 - 2 \in \mathbb{Q}[X]$, totuși $\mathbb{Q}(\sqrt[3]{2})$ nu este integral corp de descompunere al polinomului $f = X^3 - 2 \in \mathbb{Q}[X]$. Dacă descompunem $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ rezultă că corpul de descompunere al polinomului $X^3 - 2$ conține rădăcini care nu sunt în $\mathbb{Q}(\sqrt[3]{2})$. Pentru ac. motiv și înămbind în consid. Prop. 3, pentru început ne raportăm + în cercetarea leg. între subcorpurile lui F și subgrupurile lui $\text{Aut}(F)$ – în cazul cănd F este integral corp de descompunere al unui polinom.

2. Grupul Galois al unui polinom

Vom începe studiul grupului $\text{Aut}(F)$ în cazul $F = E$ este corpul de descompunere al unui polinom. Deci, fie K un corp și fie E corpul de descompunere al polinomului $f \in K[X]$.

TEOR.(a) $|\text{Aut}_K(E)| \leq |[E : K]|$ și avem egalitate dacă toate rad. lui f sunt distincte;

(b) $\text{Aut}_K(E)$ este izomorf cu un subgруp al unui груп симетрии S_n ;

(c) Dacă f este ireducibil de grad n și are toate rădăcinile distincte, atunci n divide $|\text{Aut}_K(E)|$ și $\text{Aut}_K(E)$ e izomorf cu un subgруп транзитив al lui S_n (spunem că $H \subseteq S_n$ este транзитив dacă și i, j , $1 \leq i, j \leq n$, există un $\pi \in H$ s.t. $\pi(i) = j$).

Dem. (a) Principalul instrument pe care il vom folosi este proprietatea că două corpuri de descompunere E și E' ale unui polinom $f \in K[X]$ sunt K -izomorfe. Prin inducție după $n := [E : K]$ vom arăta că numărul K -izomorfismelor $\sigma: E \rightarrow E'$ este mai mic decât $[E : K]$. Dacă $n=1$, atunci $[E : K] = 1$ impune $E = K$ și, de asemenea, $E' = E$, $\sigma = 1_K$, prin urmare $\text{Aut}_K(E) = \text{Aut}_K(K) = \langle 1_K \rangle$.

Fie $n = [E : K] > 1$ și prop. proprietatea pt. toate extinderile de grad $< n$.

Dacă $[E : K] > 1$ rezultă că f are cel puțin un factor ireductibil $p \in K[X]$ de grad > 1 . Fie $\theta \in \text{rad. a lui } p$ în E . Oricare ar fi

K -automorfismul $\sigma : E \rightarrow E'$, restricția $\sigma|_{K(\theta)} : K(\theta) \rightarrow E'$ determină un izomorfism $\tau : K(\theta) \xrightarrow{\sim} K(\theta')$, unde $\theta' = \sigma(\theta) = \tau(\theta)$. Dacă este și să se vadă că τ este unică.

In consecință, nr. K -izomorfismelor τ este egal cu nr. rad. distințe ale lui p . Deoarece $\text{grad}(p) = [K(\theta) : K]$ rezultă că nr. izomorfismelor τ este $\leq [K(\theta) : K]$, egalitatea având loc când toate rad. lui p sunt distințe. Privind diagrama

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ | & & | \\ \tau : K(\theta) & \xrightarrow{\sim} & K(\theta') \\ | & & | \\ 1_K : K & \xrightarrow{\sim} & K \end{array}$$

observăm că pt. a numără K -automorfismele σ este suficient să numărăm către diagramă de către fel sunt posibile. Astăzi, mai bine să evaluăm nr. perlungirilor unui $\tau : K(\theta) \rightarrow K(\theta')$, unde $\theta \in E$ și $\theta' \in E'$ sunt două radici ale aceluiași factor ireductibil al lui f . Deoarece $[E : K(\theta)] < n$ putem agăța ipoteza de inducție cădorile extinderii. Cf. același

nr. perlungirilor lui τ la σ este $\leq [E : K(\theta)]$, cu egalitate când f are toate rad. distințe. În plus, σ poartă proprietatea $\sigma|_K = 1_K$, deci

σ este un K -izomorfism de la E la E' . În definitiv, am obținut

relativă

$$|\text{Aut}_K(E)| \leq [E : K(\theta)] \cdot [K(\theta) : K],$$

adică $|\text{Aut}_K(E)| \leq [E : K]$, cu egalitate când pării f au radici distințe, echivalent cu f să nu aibă radici distințe. Deoarece p este un factor al lui f .

(b) Fie $\theta_1, \dots, \theta_n$ radici distințe ale lui f într-un mod de descompunere E ($1 \leq n \leq \text{grad } f$). Prop. 3 arată că orice $\sigma \in \text{Aut}_K(E)$ induce o permutare unică a mulțimii $\{\theta_1, \dots, \theta_n\}$, respectiv o permutare π_σ a mulțimii S_n . Atunci corespondența

$$\sigma \in \text{Aut}_K(E) \longmapsto \pi_\sigma \in S_n$$

delinește un monomorfism de grupuri $\text{Aut}_K E \rightarrow S_n$.

- (c) Din $|\text{Aut}_K E| = [E : K] = [E : K(\theta_1)] \cdot [K(\theta_1) : K] = [E : K(\theta_1)] \cdot \text{grad}(f) = [E : K(\theta_1)] \cdot n$ rezultă că $n \mid |\text{Aut}_K E|$. Apoi, pentru oricare $i \neq j$ elem. $\theta_i \neq \theta_j$ sunt algebrice peste $K \Rightarrow \exists$ un K -isomorfism $\sigma : K(\theta_i) \cong K(\theta_j)$ s.t. $\sigma(\theta_i) = \theta_j$. Cum σ se prelungește la un K -automorfism al lui E , rezultă că grupul $\text{Aut}_K E$ este izom. cu un subgrup transzitiv al lui S_n . ■

$\overset{E}{\text{Corpuș de descomp. al unui polinom}} f \in K[x]$ este o extindere finită a lui K . Dacă F este o extindere finită a lui K , atunci o ușoară modif. a dem. Teor. 7(a) conduce la ineq. $|\text{Aut}_K(F)| \leq [F : K]$. Cu sc. prezizare, procedem dem. ineq. $|\text{Aut}_K(F)| \leq [F : K]$ cu următ. def.

8. DEF. Fie $K \subseteq F$ o extindere finită. Se spune că F este Galois peste K și că extinderea $F \supseteq K$ este extindere Galois dacă $|\text{Aut}_K(F)| = [F : K]$. Dacă $F \supseteq K$ este extindere Galois, atunci grupul K -automorfismelor $\text{Aut}_K(F)$ este numit grupul Galois al extinderii $F \supseteq K$ și se notează $\text{Gal}(F/K)$.

9. COR. Dacă E este corpul de descompunere al unui polinom $f \in K[x]$ ce are toate răd. diferențiale (se spune că f este separabil) atunci $E \supseteq K$ este extindere Galois. În acest caz se spune că grupul Galois al corpului de descomp. este grupul Galois al polinomului f .

10. EXEMPLE.

- (a) Extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ este Galois datorită $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \langle \sigma \rangle$, unde $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ ($a, b \in \mathbb{Q}$), prin urmare $|\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.
- (b) Extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ nu este Galois, datorită $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \langle 1_{\mathbb{Q}(\sqrt[3]{2})} \rangle$: $\Rightarrow |\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.
- (c) Se cercetă dacă extinderea $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ este Galois. $\sqrt{2}$ este răd. a polin. irred (minimul) $f = x^2 - 2 \in \mathbb{Q}[x]$. Atunci $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$, și $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, cu o bază $\{\sqrt{2}\}$. Considerăm extinderea $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Aceasta este corpul de descompunere al polin. $x^2 - 3$, dacă $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ este ireductibil. În schimb, altfel ar trebui ca un element $a + b\sqrt{2}$ să fie răd. (irred). Considerăm $(a + b\sqrt{2})^2 - 3 = 0$

înseamnă $a^2 + 2b^2 = 3$ și $ab = 0$, imposibil. Deci, $X^2 - 3$ este polinomul minimal al lui $\sqrt{3}$ în c.c. în $\mathbb{Q}(\sqrt{2})$. Rezulta că $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, cu o bază $\{1, \sqrt{3}\}$. Mai departe, obținem că $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ cu o bază alcătuită din produsele elem. bazelor $\{1, \sqrt{2}\}$ și $\{1, \sqrt{3}\}$, prin urmare $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Extinderea $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ este corpul de descompunere al polinomului $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$. Orice automorfism $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ este complet determinat de acțiunile sa pe generatoare $\sqrt{2}, \sqrt{3}$. Polinomul minimal al lui $\sqrt{2}$ fiind $X^2 - 2$ rezultă că $\sigma(\sqrt{2})$ este tot o rădăcină a acestui polinom, deci $\sigma(\sqrt{2}) = \pm \sqrt{2}$. Analog, $\sigma(\sqrt{3}) = \pm \sqrt{3}$. Automorfismele posibile sunt

$$\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}, \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

Extinderea este Galois devansă $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ este corpul de descomp. al unui polinom separabil, deci autom. de mai sus sunt toate elem. grupul Galois $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q})$. Fiind grup de ordinul 4 este sau ciclic sau izomorf cu grupul lui Klein, $\mathbb{Z}_2 \times \mathbb{Z}_2$. Deoarece suntem

$$\sigma: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad și \quad \tau: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

avem $\sigma^2 = 1$ și $\tau^2 = 1$. În plus,

$$\sigma\tau(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2} \quad și \quad \sigma\tau(\sqrt{3}) = \sigma(-\sqrt{3}) = -\sqrt{3}$$

arăta că $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

În încheiere, să vedem cum lucrează σ și τ :

$$\sigma: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \longmapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},$$

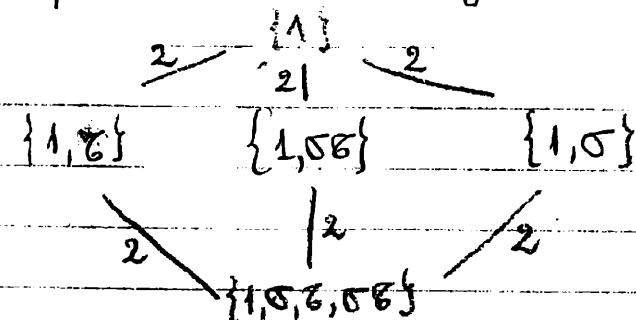
iar

$$\tau: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \longmapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}.$$

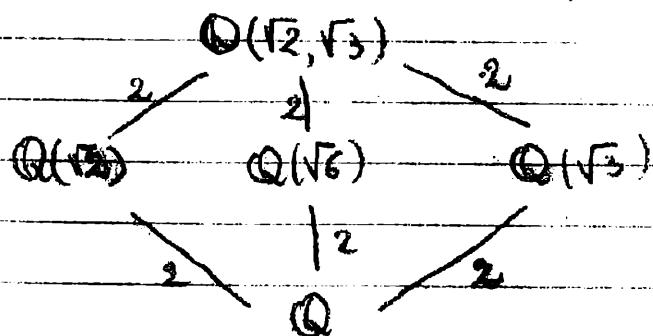
(d) Fie $E = K(\theta_1, \dots, \theta_n)$ un corp de descompunere. Unui $\sigma \in \text{Aut}_K(E)$ îi corespunde o permutare $\pi \in S_n$, dar nu și invers. De exemplu, $E = \mathbb{Q}(\sqrt{2}, i)$ este corpul de descompunere al polinomului $f = (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$, mai precis, $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i)$. Totuși, permutarea $(1, 3)$, care produce o oglindire care ducă pe $i\sqrt{2}$ în i , nu produce un element $\sigma \in \text{Aut}_{\mathbb{Q}}(E)$ devansă corpul $\sqrt{2} \mapsto i$ și $i\sqrt{2} \mapsto i^2$, adică $2 \mapsto -1$, contradicție cu ceea ce $2 \mapsto 2$. De fapt, corespondențele $\theta_i \mapsto \theta_j$ care produc K -automorisme sunt cele care permută red. același factor ireducibil din f .

Teorema fundamental a teoriei lui Galois

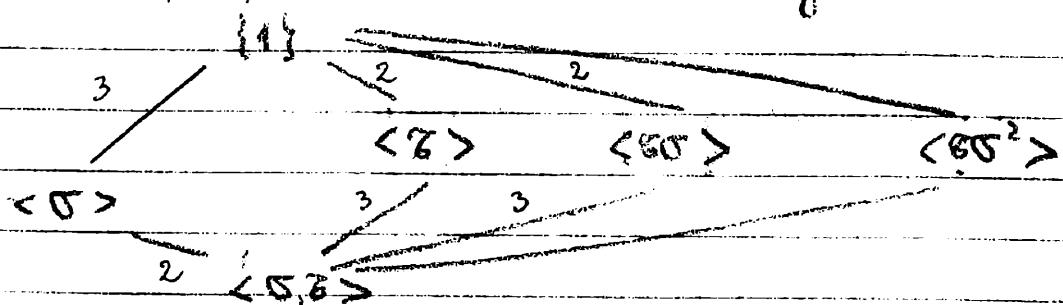
Cercetând extinderile Galois $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$ se observă o
asemănare puternică între diagrama subgroupurilor grupului
Galois $\{\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{3})\}$.



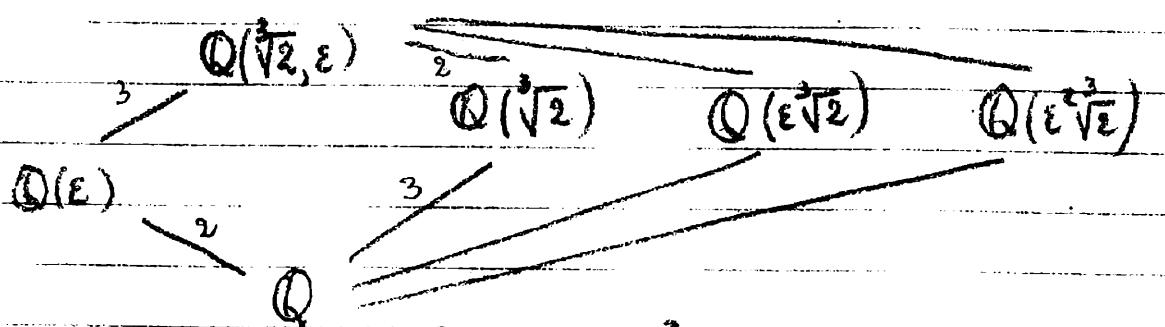
unde $\sigma: \sqrt{2} \mapsto -\sqrt{2}$ și $\delta: \sqrt{3} \mapsto -\sqrt{3}$
 și diagrama corespondență a corpuri fixate de subgrupuri



Tot o astfel de asemănare se remarcă în studiul corpului de descompunere al polinomului $x^3 - 2 \in \mathbb{Q}[x]$: dacă este nede-
cins cubici a unității, atunci cele două diagrame sunt



三



$$\text{und } \sigma : \begin{cases} \varepsilon \mapsto \varepsilon \\ \sqrt[3]{2} \mapsto \varepsilon \sqrt[3]{2} \end{cases} \quad \text{und } \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \varepsilon \mapsto \varepsilon^2 = \varepsilon \end{cases}$$

TEOREMĂ FUNDAMENTALĂ A TEORIEI LUI GALOIS. Fie $K \subseteq F$ o extindere Galois și fie $G = \text{Gal}(F/K)$ grupul Galois. Atunci există o bijectie între multimea corporilor intermedii $K \subseteq E \subseteq F$ și multimea subgrupurilor $H \subseteq G$ date de corespondențele

$$E \longmapsto H^E = \{\sigma \in G \mid \sigma(x) = x, \forall x \in E\}$$

$$K^H = \{x \in F \mid \sigma(x) = x, \forall \sigma \in H\} \longleftrightarrow H$$

care sunt inverse una celelalte. În raport cu ac. corespondență,

(1) Dacă E_1, E_2 sunt corespondențele lui H_1 , respectiv H_2 , atunci $E_1 \subseteq E_2 \iff H_2 \subseteq H_1$.

(2) $[F:E] = |H^E|$ și $[E:K] = [G:H^E]$, indexul lui H^E în G ;

$$\begin{array}{c} F \\ | \quad \{ \quad |H^E| \\ E \\ | \quad \} \quad [G:H^E] \\ K \end{array}$$

(3) $F \supseteq E$ este întărire extindere Galois, cu grupul Galois H^E .

$$\begin{array}{c} F \\ | \quad H^E \\ E \end{array}$$

(4) $E \supseteq K$ este Galois $\iff H^E$ este subgrup normal în G . În acest caz, grupul Galois $\text{Gal}(E/K)$ este izomorf cu gr. factor G/H^E :

$$\text{Gal}(E/K) \cong G/H^E.$$

Mai general, chiar dacă H^E nu este normal în G , izomorfismele lui E (într-o închidere algebraică \bar{K} a lui K ce conține pe F) care fixează pe K sunt în coresp. bij cu clasele $\{\sigma H\}$ ale lui H în G .

(5) Dacă E_1, E_2 corespund lui H_1 , respectiv H_2 , atunci intersecția $E_1 \cap E_2$ corespunde grupului $\langle H_1, H_2 \rangle$ generat de $H_1 \cup H_2$, iar corpul compozit $E_1 E_2 =$ intersecția tuturor subcorpurilor lui F care conțin despotiv pe E_1 și E_2 corespunde intersecției $H_1 \cap H_2$.

2. PROP (Criterion Eisenstein). Fie P un ideal prim în domeniul R și
 și fie $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in R[X]$, unde $n \geq 1$. Presupunem că $a_n \notin P^2$
 și a_{n-1}, \dots, a_1, a_0 sunt elemente din P , dar a_0 nu este un element în P .
 Atunci f este ireductibil în $R[X]$.

Dem. Pres. că f nu este ireductibil, să zicem $f = g \cdot h$, unde $g, h \in R[X]$
 sunt polinoame de grad ≥ 1 . Reducem modulo P și obținem ec.
~~... $\bar{a}_n X^n = \bar{g} \cdot \bar{h}$~~ în inimul de polinoame $(R/P)[X]$, unde baza înseamnă
 polinoamele cu coef. redusi modulo P . Cum P este ideal prim rezultă
 că R/P este domeniu. Atunci $\bar{a}_n X^n = \bar{g} \cdot \bar{h}$ rezultă că nici \bar{g} și nici \bar{h} nu
 au termeni libri (nemli). Aceasta înseamnă că atât g cât și h au
 termeni libri din P . Dar atunci $a_0 \in P^2$, contrad.

Criteriul Eisenstein este aplicația cel mai des a polinoamelor din $\mathbb{Z}[X]$.
 Pentru acest caz enunțul criteriului este următorul:

3. COR (Criterion Eisenstein pt. $\mathbb{Z}[X]$). Fie p un nr. prim și fie
 $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$, $n \geq 1$. Pres. că $p \nmid a_n$, $p \mid a_i$
 pt. $0 \leq i \leq n-1$, dar $p^2 \nmid a_0$. Atunci f este ired. în $\mathbb{Z}[X]$ și în $\mathbb{Q}[X]$.

Dem. Se aplică Prop. 2 cu $P = \langle p \rangle$. Deoarece f este ireductibil în $\mathbb{Z}[X]$, să se scrie $f = g \cdot h$, atunci fie $m_1 \in \mathbb{Z}$, respectiv $m_2 \in \mathbb{Z}$ multipli comuni ai coef. polinoamei f , respectiv g . Rezultă că
 $f = \frac{1}{m_1 m_2} \cdot g_1 \cdot h_1$, unde $g_1, h_1 \in \mathbb{Z}[X]$, respectiv $m_1 m_2 f = g_1 h_1$. Cu mult
 $d = m_1 m_2$ obținem $d f = g_1 h_1$. Fie $d = p_1 p_2 \cdots p_m$ și să scriem f ca produs
 a lui d . Idealul $\langle p_1 \rangle$ este prim în $\mathbb{Z}/\langle p_1 \rangle$, integrul $\Rightarrow (\mathbb{Z}/\langle p_1 \rangle)[X]$ este
 înd integrul. Reducem ecuația $d f = g_1 h_1$ modulo p_1 și obținem $\bar{0} = \bar{g}_1 \cdot \bar{h}_1$,
 de unde $\bar{g}_1 = \bar{0}$ sau $\bar{h}_1 = \bar{0}$. Deoarece de ex., $\bar{g}_1 = \bar{0}$, suntem totuși coef. liniar g_1
 se divid prim p_1 . Rezultă că $d f(x) = g_1(x) h_1(x)$ se simplifică prin
 p_1 , și devine $d_1 f(x) = g_2(x) h_2(x)$ în $\mathbb{Z}[X]$. În continuare, ecuația $d_1 f = g_2 h_2$
 se simplifică prin p_2, p_3, \dots, p_m și devine $f(x) = g'(x) h'(x)$ în $\mathbb{Z}[X]$,
 contradicție cu ipoteza f ireducibilă în $\mathbb{Z}[X]$.

4. EXEMPLE

- (a) $X^4 + 10X + 5 \in \mathbb{Z}[X]$ este ireductibil cf. crit. Eisenstein cu $p=5$.
- (b) $X^m - p \in \mathbb{Z}[X]$ este irred. pt orice prim p ($m \geq 2$).
- (c) Pt. $f = X^4 + 1 \in \mathbb{Z}[X]$ nu se poate aplica crit. Eisenstein. Consideram $g(x) = f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. Crit. Eisenstein aplicat lui g cu $p=2 \Rightarrow g$ irred. Atunci f irred, ceci daca dim $f(x) = f_1(x)f_2(x)$ rezulta $g(x) = g_1(x) \cdot g_2(x)$, unde $g_1(x) = g(x+1)$, $g_2(x) = g_2(x+1)$, ceea ce e o contrad.
- (d) $f = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X]$, p prim. Daca nu, nu se poate aplica crit. Eisenstein. Folosim nl.

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1$$

avem $f(x+1) = \frac{(x+1)^p - 1}{x} = X^{p-1} + px^{p-2} + \dots + \frac{p(p-1)}{2}X + p \in \mathbb{Z}[x]$
este irred. cf. crit. Eisenstein. Atunci $f(x)$ este irred.

5. EXEMPLE [T.F. a T.G.]

- (a) Consideram extinderea $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$.
- (i) Arith. $\omega \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ este un corp intermediar al extinderii date.
 - (ii) Identificati polin. minimal al lui $\sqrt{2} + \sqrt{3}$.
 - (iii) Arith. $\omega \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$,
 - (iv) Identificati subgrupul grupului Galois $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ care fixeaza pe $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(ii) Cu not. $\sigma: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$ si $\tau: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$ rezulta ω

$$\sigma: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\tau: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

In particular,

$$\sigma: b\sqrt{2} + c\sqrt{3} \mapsto -b\sqrt{2} + c\sqrt{3},$$

$$\tau: b\sqrt{2} + c\sqrt{3} \mapsto b\sqrt{2} - c\sqrt{3}$$

si

$$\sigma\tau = \tau\sigma: b\sqrt{2} + c\sqrt{3} \mapsto -b\sqrt{2} - c\sqrt{3}.$$

Asadar rad. polin. minimal al lui $\sqrt{2} + \sqrt{3}$ sunt $\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}$, iar polinomul minimal este

$$[X - (\sqrt{2} + \sqrt{3})][X - (\sqrt{2} - \sqrt{3})][X - (-\sqrt{2} - \sqrt{3})][X - (-\sqrt{2} + \sqrt{3})] = X^4 - 10X^2 + 1,$$

$$(iii) [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

(iv) Din (iii), $\{\varphi \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \mid \varphi(x) = x, \forall x \in \mathbb{Q}(\sqrt{2} + \sqrt{3})\}$ este automorfismul 1.

OBS. În altă călărie de a avea cu $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$: $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, și $(\sqrt{2} + \sqrt{3})^3 = (5 + 2\sqrt{6})(\sqrt{2} + \sqrt{3}) = 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2} = 9\sqrt{3} + 11\sqrt{2}$. Astfel $9\sqrt{3} + 11\sqrt{2} - 9(\sqrt{2} + \sqrt{3}) = 2\sqrt{2} \Rightarrow \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(b) Se identifică un corp de descompunere F al polinomului $X^8 - 1 \in \mathbb{Q}[X]$ și se decid că F este extindere Galois.

Rezolv. Ecuația $x^8 = 1$ are rădăcini $x_k = \cos \frac{k2\pi}{8} + i \sin \frac{k2\pi}{8}$, $k = \overline{1, 8}$, și anume $\Theta \ni x_k = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4}$ este rădăcina primitive a unității ω și $x_k = \Theta^k$, $k = \overline{1, 8}$. Deoarece $\Theta = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$ avem $\Theta^2 = i$, deci $i \in F$. Atunci $\frac{\sqrt{2}}{2}(1+i) \in F \Rightarrow \sqrt{2} \in F$, deci $F = \mathbb{Q}(\Theta, \Theta^2, \dots, \Theta^8) \cong \mathbb{Q}(\sqrt{2}, i)$. Din $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ rezultă că F este corpul de descompunere al polinomului $X^4 + 1$. $\text{grad}(X^4 + 1) = 4 \Rightarrow [F : \mathbb{Q}] = 4$. Deoarece și $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4 \Rightarrow F = \mathbb{Q}(\sqrt{2}, i)$, iar extinderea este Galois.

(c) Se identifică un corp de descompunere F al polinomului $X^8 - 2 \in \mathbb{Q}[X]$, și se decid că F este extindere Galois și se găsește grupul $\text{Aut}_{\mathbb{Q}} F$.

Rezolv. $X^8 - 2 \in \mathbb{Q}[X]$ este ireducibil.

$$x^8 - 2 = 2 \left[\left(\frac{x}{\sqrt[8]{2}} \right)^8 - 1 \right] \Rightarrow \text{rădăcini sunt } x_i = \sqrt[8]{2} \Theta^i, \quad i = \overline{1, 8}, \text{ unde}$$

$$\Theta = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \cdot \text{Deoarece } x_4 = -\sqrt{2} \Rightarrow \sqrt{2} \notin i \in F. \text{ Mai mult,}$$

$$\sqrt[8]{2}, i \in F \Rightarrow F = \mathbb{Q}(\sqrt[8]{2}, i). \text{ În definitiv, } [\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}] = 16 \text{ și}$$

$\mathbb{Q}(\sqrt[8]{2}, i)$ este corpul de descompunere al polinomului $(X^8 - 2)(X^2 + 1)$

$\mathbb{Q}(\sqrt[8]{2})(i)$

Grupul Galois este determinat de acțiunea pe generatorii $\sqrt[8]{2}$ și pe i , astfel

$$\begin{aligned} \sqrt[8]{2} &\mapsto \text{rădăcine a lui } X^8 - 2 \quad (\sqrt[8]{2} \mapsto \sqrt[8]{2} \Theta^i, \quad i = \overline{1, 8} \\ i &\mapsto \pm i \end{aligned}$$

Se definesc

$$\sigma: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \Theta \\ i \mapsto i \end{cases}$$

$$\tau: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \\ i \mapsto -i \end{cases}$$

At. cele două automorfisme pot fi completate în extensie aritm. lui θ :

$$\sigma: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \theta \\ i \mapsto i^5 \\ \theta \mapsto \theta^5 \end{cases}$$

$$\tau: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \\ i \mapsto -i \\ \theta \mapsto \frac{\sqrt[8]{2}}{2} + i \frac{\sqrt[8]{2}}{2} = \bar{\theta}^4, \end{cases}$$

$$\text{pt. că } \theta = \frac{\sqrt{2}}{2}(1+i) = \frac{(\sqrt[8]{2})^4}{2}(1+i) \rightarrow \frac{1+i}{2} \cdot (\sqrt[8]{2} \theta)^4 = \frac{1+i}{2} \cdot \sqrt{2}(-1) = -\theta = \theta^5$$

Observăm că $\text{ord}(\sigma) = 8$ și $\text{ord}(\tau) = 2$, iar automorfismele σ^i , $1 \leq i \leq 8$ și $\tau\sigma^i$, $1 \leq i \leq 8$ sunt toate distincte. De asemenea,

$$\sigma\tau = \tau\sigma^3.$$

$$\text{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1 \text{ și } \tau\sigma = \sigma^3\tau \rangle$$

Definition. If $f(x)$ is a separable polynomial over F , then the *Galois group of $f(x)$ over F* is the Galois group of the splitting field of $f(x)$ over F .

Examples

- (1) The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois with Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ where σ is the automorphism

$$\begin{aligned}\sigma : \mathbb{Q}(\sqrt{2}) &\xrightarrow{\sim} \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} &\mapsto a - b\sqrt{2}.\end{aligned}$$

- (2) More generally, any quadratic extension K of any field F of characteristic different from 2 is Galois. This follows from the discussion of quadratic extensions following Corollary 13.13, which shows that any extension K of degree 2 of F (where the characteristic of F is not 2) is of the form $F(\sqrt{D})$ for some D hence is the splitting field of $x^2 - D$ (since if $\sqrt{D} \in K$ then also $-\sqrt{D} \in K$).
(3) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since its group of automorphisms is only of order 1.
(4) The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over \mathbb{Q} since it is the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)$. Any automorphism σ is completely determined by its action on the generators $\sqrt{2}$ and $\sqrt{3}$, which must be mapped to $\pm\sqrt{2}$ and $\pm\sqrt{3}$, respectively. Hence the only possibilities for automorphisms are the maps

$$\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

Since the Galois group is of order 4, all these elements are in fact automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} .

Define the automorphisms σ and τ by

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

or, more explicitly, by

$$\begin{aligned}\sigma : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \tau : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}\end{aligned}$$

(since, for example,

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = (-\sqrt{2})(\sqrt{3}) = -\sqrt{6}.$$

Then $\sigma^2(\sqrt{2}) = \sigma(\sigma\sqrt{2}) = \sigma(-\sqrt{2}) = \sqrt{2}$ and clearly $\sigma^2(\sqrt{3}) = \sqrt{3}$. Hence $\sigma^2 = 1$ is the identity automorphism. Similarly, $\tau^2 = 1$. The automorphism $\sigma\tau$ can be easily computed:

$$\sigma\tau(\sqrt{2}) = \sigma(\tau(\sqrt{2})) = \sigma(\sqrt{2}) = -\sqrt{2}$$

and

$$\sigma\tau(\sqrt{3}) = \sigma(\tau(\sqrt{3})) = \sigma(-\sqrt{3}) = -\sqrt{3}$$

so that $\sigma\tau$ is the remaining nontrivial automorphism in the Galois group. Since this automorphism also evidently has order 2 in the Galois group, we have

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$$

i.e., the Galois group is isomorphic to the Klein 4-group.

Associated to each subgroup of $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is the corresponding fixed subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. For example, the subfield corresponding to $\{1, \sigma\tau\}$ is the set of elements fixed by the map

$$\sigma\tau : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

which is the set of elements $a + d\sqrt{6}$, i.e., the field $\mathbb{Q}(\sqrt{6})$. One can similarly determine the fixed fields for the other subgroups of the Galois group:

subgroup	fixed field
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	\mathbb{Q}

- (5) The splitting field of $x^3 - 2$ over \mathbb{Q} is Galois of degree 6. The roots of this equation are $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ where $\rho = \xi_3 = \frac{-1 + \sqrt{-3}}{2}$ is a primitive cube root of unity. Hence the splitting field can be written $\mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2})$. Any automorphism maps each of these two elements to one of the roots of $x^3 - 2$, giving 9 possibilities, but since the Galois group has order 6 not every such map is an automorphism of the field.

To determine the Galois group we use a more convenient set of generators, namely $\sqrt[3]{2}$ and ρ . Then any automorphism σ maps $\sqrt[3]{2}$ to one of $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$ and maps ρ to ρ or $\rho^2 = \frac{-1 - \sqrt{-3}}{2}$ since these are the roots of the cyclotomic polynomial $\Phi_3(x) = x^2 + x + 1$. Since σ is completely determined by its action on these two elements this gives only 6 possibilities and so each of these possibilities is actually an automorphism. To give these automorphisms explicitly, let σ and τ be the automorphisms defined by

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \quad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1 - \rho. \end{cases}$$

As before, these can be given explicitly on the elements of $\mathbb{Q}(\sqrt[3]{2}, \rho)$, which are linear combinations of the basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \rho, \rho\sqrt[3]{2}, \rho(\sqrt[3]{2})^2\}$. For example

$$\begin{aligned} \sigma(\rho\sqrt[3]{2}) &= (\rho)(\rho\sqrt[3]{2}) = \rho^2\sqrt[3]{2} = (-1 - \rho)\sqrt[3]{2} \\ &= -\sqrt[3]{2} - \rho\sqrt[3]{2} \end{aligned}$$

and we may similarly determine the action of σ on the other basis elements. This gives

$$\begin{aligned} \sigma : \quad a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\rho + e\rho\sqrt[3]{2} + f\rho\sqrt[3]{4} &\mapsto \\ a - e\sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\rho + (b - e)\rho\sqrt[3]{2} - cp\sqrt[3]{4}. & \end{aligned} \tag{14.1}$$

The other elements of the Galois group are

$$1 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \quad \sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho^2\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases}$$

$$\tau\sigma : \begin{cases} \sqrt[3]{2} \mapsto \rho^2 \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases} \quad \tau\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto \rho \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

Computing $\sigma\tau$ we have

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \xrightarrow{\tau} \sqrt[3]{2} \xrightarrow{\sigma} \rho \sqrt[3]{2} \\ \rho \xrightarrow{\tau} \rho^2 \xrightarrow{\sigma} \rho^2 \end{cases}$$

i.e.,

$$\sigma\tau : \begin{cases} \sqrt[3]{2} \mapsto \rho \sqrt[3]{2} \\ \rho \mapsto \rho^2 \end{cases}$$

so that $\sigma\tau = \tau\sigma^2$. Similarly one computes that $\sigma^3 = \tau^2 = 1$. Hence

$$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \{\sigma, \tau\} \cong S_3$$

is the symmetric group on 3 letters. Alternatively (and less computationally), since $G = \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ acts as permutations of the 3 roots of $x^3 - 2$, G is a subgroup of S_3 , hence must be S_3 since it is of order 6. The computations above explicitly identify the automorphisms in G and give an explicit isomorphism of G with S_3 .

As in the previous example we can determine the fixed fields for any of the subgroups of the Galois group. For example, consider the fixed field of the subgroup $\{1, \sigma, \sigma^2\}$ generated by σ . These are just the elements fixed by σ (given explicitly in equation (1)) since if an element is fixed by σ then it is also fixed by σ^2 . (In general, the fixed field of some subgroup is the field fixed by a set of generators for the subgroup.) The elements fixed by σ are those with

$$a = a \quad b = -e \quad c = f - e \quad d = d \quad e = b - e \quad f = -c$$

which is equivalent to $b = c = f = e = 0$. Hence the fixed field of $\{1, \sigma, \sigma^2\}$ is the field $\mathbb{Q}(\rho)$.

Remark: This example shows that some care must be exercised in determining Galois groups from the actions on generators. As mentioned, not every map taking $\sqrt[3]{2}$ and $\rho \sqrt[3]{2}$ to roots of $x^3 - 2$ gives rise to an automorphism of the field (for example, the map

$$\begin{aligned} \sqrt[3]{2} &\mapsto \rho \sqrt[3]{2} \\ \rho \sqrt[3]{2} &\mapsto \rho^2 \sqrt[3]{2} \end{aligned}$$

clearly cannot be an automorphism since it is evidently not an injection). The point is that there may be (sometimes very subtle) algebraic relations among the generators and these relations must be respected by an automorphism. For example, the quotient of the generators here is ρ , which is mapped to 1 and not to a root of the minimal polynomial for ρ . Put another way, the quotient of these generators satisfies a quadratic equation and this map does not respect that property.

For another (less trivial) example, compare with the discussion of the splitting field of $x^8 - 2$ in Section 2.

- (6) As in Example 3, the field $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over \mathbb{Q} since any automorphism is determined by where it sends $\sqrt[4]{2}$ and of the four possibilities $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, only two are elements of the field (the two real roots).

Note that we have

$$\begin{array}{ccccccc} & & & 4 & & & \\ & & \overbrace{\quad\quad\quad}^4 & & & & \\ \mathbb{Q} & \subset & \mathbb{Q}(\sqrt{2}) & \subset & , & \mathbb{Q}(\sqrt[4]{2}) & \\ & & \underbrace{\quad\quad\quad}_2 & & & & \underbrace{\quad\quad\quad}_2 \end{array}$$

where $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are both Galois extensions by Example 2 since both are quadratic extensions. This shows that a Galois extension of a Galois extension is not necessarily Galois.

- (7) The extension of finite fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ constructed after Proposition 13.37 is Galois by Corollary 6 since \mathbb{F}_{p^n} is the splitting field over \mathbb{F}_p of the separable polynomial $x^{p^n} - x$. It follows that the group of automorphisms for this extension is of order n . The injective homomorphism

$$\begin{aligned} \sigma : \mathbb{F}_{p^n} &\rightarrow \mathbb{F}_{p^n} \\ \alpha &\mapsto \alpha^p \end{aligned}$$

of Proposition 13.35 is surjective in this case since \mathbb{F}_{p^n} is finite, hence is an isomorphism. This gives an automorphism of \mathbb{F}_{p^n} , called the *Frobenius* automorphism, which we shall denote by σ_p . Iterating σ_p we have $\sigma_p^2(\alpha) = \sigma_p(\sigma_p(\alpha)) = (\alpha^p)^p = \alpha^{p^2}$. Similarly we have

$$\sigma_p^i(\alpha) = \alpha^{p^i} \quad i = 0, 1, 2, \dots$$

Since $\alpha^{p^n} = \alpha$, we see that $\sigma_p^{p^n} = 1$ is the identity automorphism. No lower power of σ_p can be the identity, since this would imply $\alpha^{p^i} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$ for some $i < n$, which is impossible since there are only p^i roots of this equation. It follows that σ_p is of order n in the Galois group, which means that $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n , with the Frobenius automorphism σ_p as generator.

- (8) The inseparable extension $\mathbb{F}_2(x)$ over $\mathbb{F}_2(t)$ where $x^2 - t = 0$ considered in Section 13.5 is not Galois. Any automorphism of this degree 2 extension is determined by its action on x , which must be sent to a root of the equation $x^2 - t$. We have already seen that there is only one root of this equation (with multiplicity 2) since we are in a field of characteristic 2. Hence the extension has only the trivial automorphism. Note that $\mathbb{F}_2(x)$ is the splitting field for $x^2 - t$ over $\mathbb{F}_2(t)$, so this example shows the separability condition in Corollary 6 is necessary.

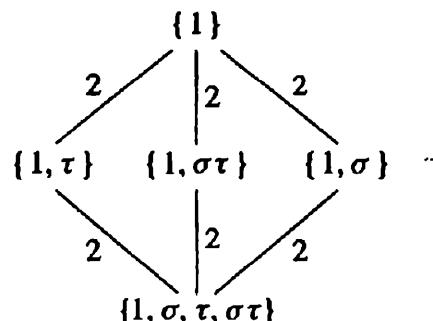
EXERCISES

- (a) Show that if the field K is generated over F by the elements $\alpha_1, \dots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K .
- (b) Let $G \leq \text{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \dots, \sigma_k$ are generators for G . Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \dots, \sigma_k$.

2. Let τ be the map $\tau : \mathbb{C} \rightarrow \mathbb{C}$ defined by $\tau(a + bi) = a - bi$ (*complex conjugation*). Prove that τ is an automorphism of \mathbb{C} .
3. Determine the fixed field of complex conjugation on \mathbb{C} .
4. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.
5. Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.
6. Let k be a field.
 - (a) Show that the mapping $\varphi : k[t] \rightarrow k[t]$ defined by $\varphi(f(t)) = f(at + b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k .
 - (b) Conversely, let φ be an automorphism of $k[t]$ which is the identity on k . Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\varphi(f(t)) = f(at + b)$ as in (a).
7. This exercise determines $\text{Aut}(\mathbb{R}/\mathbb{Q})$.
 - (a) Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.
 - (b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m . Conclude that σ is a continuous map on \mathbb{R} .
 - (c) Prove that any continuous map on \mathbb{R} which is the identity on \mathbb{Q} is the identity map, hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.
8. Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the *fractional linear transformations* determined by $t \mapsto \frac{at + b}{ct + d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$ (so $f(t) \in k(t)$ maps to $f(\frac{at + b}{ct + d})$) (cf. Exercise 18 of Section 13.2).
9. Determine the fixed field of the automorphism $t \mapsto t + 1$ of $k(t)$.
10. Let K be an extension of the field F . Let $\varphi : K \rightarrow K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K' . Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\text{Aut}(K/F) \xrightarrow{\sim} \text{Aut}(K'/F')$.

14.2 THE FUNDAMENTAL THEOREM OF GALOIS THEORY

In the Galois extension $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ considered in the previous section, there was a strong similarity between the diagram of subgroups of the Galois group:



and the diagram of corresponding fixed fields