CAPITOLUL 4

VALORI ŞI VECTORI PROPRII. FORME CANONICE ALE MATRICELOR ŞI ENDOMORFISMELOR

4.1. Forma celular diagonală - definiție

Fie K un corp comutativ şi V un spațiu vectorial peste K de dimensiune n. Notăm cu $End_K(V)$ mulțimea endomorfismelor pe V, adică mulțimea transformărilor liniare u: $V \to V$.

Definiție4.1.1. *Un subspațiu vectorial L al spațiului vectorial V se numeşte subspațiu invariant la aplicația liniară u : $V \to V$ dacă $u(x) \in L$ pentru orice $x \in L$. Un subspațiu L invariant la aplicația liniară u : $V \to V$ se numeşte indecompozabil (relativ la u) dacă nu poate fi reprezentat ca suma directă a două subspații diferite de $\{0_V\}$ invariante la u.*

Fie $L \subset V$ un subspațiu de dimensiune p invariant la aplicația liniară u : $V \to V$. Fie B' = $\{e_1, e_2, \ldots, e_p\}$ o bază a lui L şi B = $\{e_1, e_2, \ldots, e_p, \ldots, e_n\}$ o bază a lui V obținută prin completarea lui B'. Considerăm *aplicația liniară indusă de u pe L*, adică aplicația u' : $L \to L$, $u'(x) = u(x)$ pentru orice $x \in L$ (u' este corect definită deoarece L este un subspațiu invariant). Notăm cu $M_B(u) = (a_{ij})_{1\le i,j\le n}$ matricea lui u în baza B. Deci pentru orice $i \in \{1,2, \ldots, n\}$

$$u(e_i) = \sum_{i=1}^{n} a_{ij} e_j .$$

Deoarece pentru orice $i \in \{1,2, \ldots, p\}$ $u(e_i) \in L = Sp(B')$, rezultă că

$$u(e_i) = \sum_{i=1}^{p} a_{ij} e_j$$

şi deci $a_{ij} = 0$ pentru orice $j>p$. Ca urmare, matricea $M_B(u)$ este de forma:

$$M_B(u) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1p} & 0 & \ldots & 0 \\ a_{21} & a_{22} & \ldots & a_{2p} & 0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{p1} & a_{p2} & \ldots & a_{pp} & 0 & \ldots & 0 \\ a_{p+1,1} & a_{p+1,2} & \ldots & a_{p+1,p} & a_{p+1,p+1} & \ldots & a_{p+1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,p} & a_{n,p+1} & \ldots & a_{n,n} \end{pmatrix}$$

$$M_B(u) = \begin{pmatrix} M_{B'}(u') & O \\ A & A' \end{pmatrix}$$

Vom demonstra că V se reprezintă în mod unic (până la un izomorfism între perechi de sumanzi) ca sumă directă de un număr finit de subspaţii $L_1, L_2, \ldots, L_q$ indecompozabile relativ la u:

$V = L_1 \oplus L_2 \oplus \ldots \oplus L_q$, L_i subspaţiu invariant la u pentru orice i.

Pentru fiecare $i \in \{1, 2, ..q\}$ notăm cu u_i aplicaţia indusă de u pe L_i şi considerăm o bază B_i pentru L_i. Este uşor de observat că $B = \bigcup_{i=1}^{q} B_i$ este o bază a lui V. Notăm cu $M_{B_i}(u_i)$ matricea asociată lui u_i în baza B_i pentru fiecare $i \in \{1,2, \ldots, q\}$. Ţinând cont că pentru orice $i \in \{1,2, \ldots, q\}$ şi orice $e \in B_i$ $u(e) \in L_i = Sp(B_i)$, rezultă că matricea lui u în baza $B = \bigcup_{i=1}^{q} B_i$ este de forma

$$M_B(u) = \begin{pmatrix} M_{B_1}(u_1) & & & \\ & M_{B_2}(u_2) & & O \\ & & \ddots & \\ O & & & M_{B_q}(u_q) \end{pmatrix}$$

care se numeşte *formă celular diagonală*.

Astfel se reduce studiul lui u la studiul transformărilor liniare

$$u_i : L_i \to L_i,\ i \in \{1, 2, \ldots, q\}.$$

4.2. Inele şi module

Definiţia 4.2.1. *Se numeşte inel o mulţime nevidă R înzestrată cu două operaţii, una notată aditiv* +: R×R→R *(numită adunare) şi cealaltă notată multiplicativ* ·: R×R→R *(numită înmulţire),care satisfac următoarele condiţii*

1. *R este grup abelian faţă de operaţia de adunare*
2. *operaţia de înmulţire este asociativă*
3. *oricare ar fi $x,y,z \in R$, avem*

$$x\,(y + z) = xy + xz$$

$$(x + y\,)z = xz + yz.$$

Dacă R este un inel, grupul abelian R faţă de adunare se numeşte *grupul aditiv subiacent inelului*. Elementul neutru faţă de adunare se notează cu 0 şi se numeşte *elementul zero* al inelului, iar *opusul* faţă de adunare al unui element oarecare $x \in R$ se notează cu $-x$. Dacă, în plus, operaţia de înmulţire admite element neutru, spunem că inelul este *unitar*. Elementul neutru la înmulţire (dacă există) se notează cu 1 şi se numeşte *elementul unitate* al inelului. Dacă înmulțirea este comutativă, inelul se numeşte *comutativ*. Spunem că $x \in R$ este *divizor al lui zero la stânga* (respectiv *la dreapta*) dacă există $y \in R$, $y \neq 0$ astfel încât $xy = 0$ (respectiv $yx = 0$). Un element care este în acelaşi timp divizor al lui zero la stânga şi la dreapta se numeşte simplu, *divizor la lui zero*. Un inel unitar nenul fără divizori ai lui zero la stânga şi la dreapta nenuli se numeşte *inel integru*. Dacă, în plus, inelul este şi comutativ el se numeşte *domeniu de integritate*. Elementele inversabile față de operația de înmulțire a unui inel unitar R se numesc *elemente inversabile ale inelului*, iar mulțimea lor se notează cu U(R) (este uşor de arătat că U(R) are o structură de grup față de operația de înmulțire din R). Dacă $U(R) = R-\{0\}$, atunci R este corp. Dacă a şi b sunt două elemente din domeniul de integritate R, se spune că a *divide* b şi se scrie $a|b$ dacă există $c \in R$ astfel încât $b = ac$. Două elemente a şi b din R se numesc *asociate în divizibilitate* dacă $a|b$ şi $b|a$, sau echivalent dacă există un element $u \in U(R)$ astfel încât $b = ua$. Dacă a şi b sunt asociate în divizibilitate, atunci scriem $a \sim b$. Un element $d \in R$ se numeşte *cel mai mare divizor comun* al elementelor a şi b din R dacă are următoarele proprietăți:

1. $d|a$ şi $d|b$
2. dacă $d'|a$ şi $d'|b$, atunci $d'|d$.

Orice două elemente d_1 şi d_2 din R (domeniu de integritate) care satisfac condițiile 1 şi 2 de mai sus sunt asociate în divizibilitate. De aceea vom nota cu (a, b) orice element care este cel mai mare divizor comun al lui a şi b (adică nu facem distincție între elementele asociate în divizibilitate). Două elemente a şi b din R se numesc *prime între ele* dacă 1 este cel mai mare divizor comun al lui a şi b. Un element x dintr-un domeniu de integritate R se numeşte *ireductibil* dacă $x \neq 0$, $x \notin U(R)$, şi în plus dacă din $x = ab$ rezultă a sau b inversabil. Un element $p \in R$ se numeşte *prim* dacă $p \neq 0$, $p \notin U(R)$, şi în plus, dacă din $p|ab$ rezultă că $p|a$ sau $p|b$. Într-un domeniu de integritate orice element prim este ireductibil. Dacă în plus, pentru orice două elemente există un cel mai mare divizor comun, atunci orice element ireductibile este prim (teorema 1.8/pg. 212 [5]). Un domeniu de integritate R se numeşte *factorial* dacă orice element nenul şi neinversabil al lui R este produs de elemente prime ale lui R. Într-un inel factorial pentru orice două elemente a şi b există un cel mai mare divizor comun (este dat de produsul elementelor prime comune la puterea minimă la care apar în descompunerile lui a şi b).

Exemplul 4.2.2. *Fie R un inel comutativ şi unitar şi m şi n două numere naturale nenule. Se numeşte matrice de tip (m,n) peste inelul R, orice funcţie*

$$A: \{1,2,\ldots,m\} \times \{1,2,\ldots,n\} \rightarrow R.$$

Oricărei matrice A de tipul (m,n) peste inelul R i se asociază un tablou cu m linii şi n coloane

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

unde $a_{ij} = A(i,j)$ *pentru* $1 \leq i \leq m$ *şi* $1 \leq j \leq n$.

Reciproc, un astfel de tablou cu m linii şi n coloane de elemente (coeficienţi) din inelul R, determină în mod unic o matrice A, dată prin $A(i,j) = a_{ij}$ *pentru* $1 \leq i \leq m$ *şi* $1 \leq j \leq n$. *În cele ce urmează vom scrie matricea A sub forma unui astfel de tablou sau condensat, A =*

$\left(a_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}}$ *(sau A = $(a_{ij})_{i,j}$ dacă m şi n se subînțeleg). Vom nota cu $M_{m,n}(R)$ mulțimea matricelor cu m linii şi n coloane cu elemente din R. Vom defini pe $M_{m,n}(R)$ o operație algebrică internă, numită adunarea matricelor, în felul următor:*

dacă $A = (a_{ij})_{i,j}\in M_{m,n}(R), B=(b_{ij})_{i,j}\in M_{m,n}(R)$, *atunci* $A+B = C$, *unde*

$C=(c_{ij})_{i,j} \in M_{m,n}(R)$ *şi* $c_{ij} = a_{ij} + b_{ij}$ *pentru orice* $1\le i\le m$ *şi* $1\le j\le n$.

Produsul AB a două matrice $A = (a_{ij})_{i,j}\in M_{m,n}(R)$ *şi* $B=(b_{ij})_{i,j}\in M_{n,p}(R)$ *este o matrice* $C=(c_{ij})_{i,j} \in M_{m,p}(R)$ *pentru care*

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \text{ pentru orice } 1\le i\le m \text{ şi } 1\le j\le p.$$

Transpusa unei matrice $A=\left(a_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}}$, *este o matrice notată* $A^t = \left(a^t_{ij}\right)_{\substack{1\le i\le n\\ 1\le j\le m}}$, *ale cărei elemente sunt:* $a^t_{ij} = a_{ji}$ *pentru orice* $1\le i\le n$, $1\le j\le m$. *O matrice pentru care m=n se numeşte pătratică. Matricele pătratice pentru care* $A=A^t$ *se numesc matrice simetrice. Mulțimea matricelor pătratice* $M_{n,n}(R)$ *cu elemente din inelul comutativ şi unitar R are o structură de inel unitar în raport cu adunarea şi înmulțirea matricelor. Elementul neutru la înmulțire în* $M_{n,n}(R)$ *este matricea ale cărei elemente sunt egale cu elementul zero al inelului R, cu excepția celor de pe diagonala principală care sunt egale cu 1 (elementul unitate al inelului R). Ea se notează cu* I_n:

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

Determinantul unei matrice $A = (a_{ij})_{ij} \in M_{n,n}(R)$ *se notează cu* $det(A)$ *sau*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

şi se defineşte ca $\sum_{\sigma \in S_n} \varepsilon_\sigma a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} \in R$ *(suma se face după toate permutările* σ *ale mulțimii* $\{1, 2, \ldots, n\}$*, iar* ε_σ *reprezintă signatura permutării* σ*). În particular,*

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Pentru orice matrice $A = (a_{ij})_{ij} \in M_{n,n}(R)$*, elementul* $\Gamma_{ij} = (-1)^{i+j} det(A_{ij}) \in R$ *se numeşte complementul algebric al elementului* a_{ij}*, unde* A_{ij} *este matricea ce se obține din A eliminând linia i şi coloana j. Se poate arăta că*

$$det(A) = \sum_{j=1}^{n} a_{ij}\Gamma_{ij} \text{ pentru orice } 1 \le i \le n.$$

Determinanții au următoarele proprietăți (corolar 1.8/pg 162 [4], propoziția 1.10/pg 163 [4]):

1. $det(A) = det(A^t)$ *pentru orice matrice* $A \in M_{n,n}(R)$.
2. *O matrice cu două coloane egale are determinantul zero.*
3. *Dacă permutăm două coloane, determinantul matricei îşi schimbă semnul.*
4. *Dacă la o coloană a matricei se adună o altă coloană înmulțită cu un element* $a \in R$*, determinantul matricei nu se schimbă.*
5. *Dacă toate elementele unei coloane sunt egale cu zero, atunci determinantul matricei este zero.*

6. $det(AB) = det(A)det(B)$ pentru orice $A,B \in M_{n,n}(R)$.

Datorită faptului că $det(A) = det(A^t)$, este adevărată şi lista de proprietăţi ce se obţine înlocuind în 2-5 cuvântul coloană cu cuvântul linie.

Grupul unităţilor inelului $M_{n,n}(R)$ (mulţimea elementelor inversabile în inelul $M_{n,n}(R)$) se notează cu $GL_n(R)$ şi se numeşte grupul liniar de grad n al inelului R. În particular, $GL_1(R) = U(R)$. Se demonstrează că o matrice $A \in GL_n(R)$ (adică este inversabilă) dacă şi numai dacă $det(A) \in U(R)$ (teorema 3.1/pg. 166 [4]). Demonstraţia este constructivă: A^{-1}(inversa matricei A) se obţine din matricea reciprocă a lui A prin înmulţirea tuturor elementelor cu inversul determinantului lui A. Reciproca matricei $A = (a_{ij})_{ij}$ este transpusa matricei $(\Gamma_{ij})_{ij}$, unde Γ_{ij} reprezintă complementul algebric al lui a_{ij}.

Se numeşte submatrice a matricei $A \in M_{m,n}(R)$ o matrice obţinută din A prin eliminarea unor linii şi unor coloane. Determinantul unei submatrice cu p linii (şi p coloane) se numeşte minor de ordin p al matricei A. Se spune că matricea A are rangul r, dacă A are un minor nenul de ordin r şi toţi minorii lui A de ordin r+1 sunt nuli.

Exemplul 4.2.3. *Fie R un inel comutativ şi unitar. Considerăm mulţimea şirurilor $(a_0, a_1, \ldots a_n, \ldots)$ de elemente din inelul R, cu condiţia ca în fiecare şir, începând de la un anumit rang, componentele să fie 0 (elementul zero al inelului R). Un astfel de şir se numeşte polinom cu coeficienţi în R (elementele $a_0, a_1, \ldots a_n, \ldots$ se numesc coeficienţii polinomului). Definim adunarea polinoamelor prin*

$$(a_0, a_1, \ldots a_n, \ldots)+(b_0, b_1, \ldots b_n, \ldots)$$
$$=(a_0 + b_0, a_1 + b_n, \ldots a_n+ b_n, \ldots)$$

Dacă $P = (a_0, a_1, \ldots a_n, \ldots)$ şi $Q = (b_0, b_1, \ldots b_n, \ldots)$ produsul PQ este polinomul $S =(c_0, c_1, \ldots c_n, \ldots)$ cu proprietatea că $c_k = \sum_{i+j=k} a_i b_j$ pentru orice $k \geq 0$. Mulțimea polinoamelor cu coeficienți din inelul comutativ şi unitar R are o structură de inel comutativ şi unitar în raport cu adunarea şi înmulțirea definite mai sus. Elementele inelului R pot fi privite ca polinoame cu coeficienți în R prin identificarea unui element $a \in R$ cu polinomul $(a, 0, \ldots, 0, \ldots)$. Dacă $P= (a_0, a_1, \ldots a_n, \ldots)$ este un polinom nenul, atunci $n = \max\{i, a_i \neq 0\}$ se numeşte gradul polinomului P, şi se notează cu grad(P). Pentru polinomul nul $(0, \ldots,0,\ldots)$ convenim să considerăm gradul său ca fiind $-\infty$. Coeficientul a_n, unde $n=grad(P)$ (P nenul) se numeşte coeficientul dominant al polinomului P. Dacă acest coeficient a_n este 1 (elementul unitate al inelului R) atunci P se numeşte polinom unitar. Dacă P şi Q sunt două polinoame cu coeficienți în R, atunci $grad(P+Q) \leq \max(grad(P), grad(Q))$ şi $grad(PQ) \leq grad(P) + grad(Q)$. Mai mult, dacă P şi Q sunt nenule şi coeficienții dominanți ai lui P şi Q nu sunt divizori ai lui zero, atunci $grad(PQ) \leq grad(P) + grad(Q)$.

Notăm prin X polinomul $(0,1,0,\ldots,0,\ldots)$ care se numeşte nedeterminata X. Înmulțirea polinoamelor ne dă

$$X^2 = XX =(0, 0, 1, 0, \ldots, 0,\ldots)$$

şi, mai general, pentru orice număr natural i

$$X^i =(\underbrace{0, \ldots 0}_{i \text{ ori}}, 1, 0, \ldots, 0, \ldots)$$

Folosind adunarea şi înmulțirea definite pe mulțimea polinoamelor cu coeficienți în R se obține că orice polinom $P= (a_0, a_1, \ldots a_n, \ldots)$ poate fi scris sub forma

$$P = a_0 + a_1X + \ldots + a_mX^m,\ unde\ m = grad(P).$$

Elementele a_0, a_1, …a_m poartă denumirea de coeficienți ai polinomului P. Inelul polinoamelor cu coeficienți în R se notează cu R[X]. Un element $a\in R$ este inversabil în R dacă şi numai dacă a (privit ca polinom) este inversabil în R[X]. Dacă, în plus, R este domeniu de integritate, atunci R[X] este domeniu de integritate şi U(R) = U(R[X]).

Definiția 4.2.4. *Fie R un inel şi $I\subset R$ o submulțime nevidă a sa. Spunem că I este un ideal la stânga (respectiv la dreapta) al inelului B dacă:*

1. *oricare ar fi x, y $\in I$, rezultă x - y$\in I$*
2. *oricare ar fi $a\in R$ şi $x\in I$, rezultă $ax\in I$ (respectiv $xa\in I$).*

Un ideal care este în acelaşi timp ideal la stânga şi la dreapta se numeşte ideal bilateral.

Dacă inelul R este inel comutativ, atunci este clar că noțiunile de ideal la stânga, ideal la dreapta şi ideal bilateral coincid. În acest caz vom spune simplu *ideal* al inelului R.

Dacă R este un inel unitar şi a∈ R, atunci

1. Ra = {xa, x∈ R} este ideal la stânga în R
2. aR ={ax, x∈ R} este ideal la dreapta în R
3. aRa ={ $\sum_{i=1}^{n} x_i a y_i$, x_i, y_i ∈ R, i =1,2, ..n} este ideal bilateral în R.

Dacă R este un inel unitar şi a∈ R, atunci aR, Ra, aRa se numesc *ideale principale*, respectiv, la stânga, la dreapta şi bilateral. Un inel se numeşte *principal* dacă este un domeniu de integritate şi orice ideal al său este principal. Dacă R este un inel principal, atunci R este factorial (teorema 4.1/pg. 218 [5]). Dacă R este un inel principal, a, b$\in$R şi d este un cel mai mare divizor comun al elementelor a şi b, atunci există u, v$\in$R astfel încât d = ua + vb (este suficient să observăm că Ra + Rb este un ideal în inelul principal R, deci există $d_1 \in R$ astfel încât $Rd_1 = Ra + Rb$; este uşor de observat că d_1 este cel mai mare divizor comun pentru a şi b, deci este asociat în divizibilitate cu d). În particular, elementele a şi b sunt prime între ele dacă şi numai dacă există elementele u şi v astfel încât ua + vb = 1.

Un domeniu de integritate R se numeşte *inel euclidian* dacă există o funcție $\varphi : R- \{0\} \to \mathbf{N}$ având proprietatea că oricare ar fi a, b$\in$R, b$\neq$0, există q, r $\in$ R astfel încât

$$a = bq + r, \text{ unde } r = 0 \text{ sau } \varphi(r) < \varphi(b) \text{ (formula împărțirii cu rest).}$$

Dacă R este un inel euclidian, atunci R este un inel principal (teorema 4.4/pg. 219 [5]). În cazul unui inel euclidian se poate determina cel mai mare divizor comun a două elemente prin aplicarea algoritmului lui Euclid (se aplică de un număr finit de ori formula împărțirii cu rest).Un exemplu de inel euclidian este inelul numerelor întregi **Z**. În acest inel are loc formula împărțirii cu rest: dacă a, b$\in$**Z**, b$\neq$0, atunci există q, r$\in$**Z** unic determinate cu proprietatea

$$a = bq + r, \text{ unde } 0 \leq r < |b|.$$

Evident, **Z** este un inel euclidian, considerând funcția:

$$\varphi : \mathbf{Z}-\{0\} \to \mathbf{N}, \varphi(n) = |n| \text{ (modulul lui n).}$$

Un alt exemplu de inel euclidian este inelul K[X] al polinoamelor cu coeficienți în corpul comutativ K. În cadrul acestui inel se poate demonstra teorema împărțirii cu rest: oricare ar fi polinoamele P_1, $P_2 \in$ K[X] cu $P_2 \neq 0$, există două polinoame Q şi R astfel încât

$$P_1 = P_2Q + R, \text{ unde } grad(R) < grad(P_2).$$

Pentru a arăta că K[X] este inel euclidian, considerăm funcţia

$$\varphi: K[X] - \{0\} \to \mathbf{N}, \varphi(P) = grad(P).$$

Deci inelul K[X] (K corp comutativ) este euclidian, şi în consecinţă este principal. De asemenea fiind principal este factorial.

Definiţie 4.2.5. *Fie R şi S două inele. Se numeşte morfism de la R la S o funcţie $\varphi : R \to S$, care îndeplineşte următoarele condiţii:*

1. *$\varphi(x+y) = \varphi(x) + \varphi(y)$ oricare ar fi x, $y \in R$*
2. *$\varphi(xy) = \varphi(x)\varphi(y)$ oricare ar fi x, $y \in R$.*

Un morfism $\varphi : R \to S$, unde R şi S sunt inele unitare, care satisface în plus condiţia $\varphi(1) = 1$ se numeşte *morfism unitar de inele*. Un morfism de inele $\varphi : R \to S$ care, în plus, este bijectiv se numeşte *izomorfism de inele*. Se poate arăta că dacă $\varphi : R \to S$ este izomorfism de inele, atunci şi $\varphi^{-1} : S \to R$ este izomorfism de inele. Dacă

$$\varphi : R \to S$$

este un morfism de inele atunci

1. Ker $\varphi = \{x \in R: \varphi(x) = 0\}$ este un ideal bilateral al lui R numit *nucleul morfismului* φ.
2. Im $\varphi = \varphi/R) = \{\varphi(x), x \in R\}$ este un subinel al lui S (împreună cu operaţiile induse de cele două operaţii algebrice de pe S formează un inel) numit *imaginea morfismului* φ.

Un modul se deosebeşte de un spaţiu vectorial doar prin faptul că înmulţirea externă nu se face cu elementele unui corp (ca în cazul spaţiilor vectoriale), ci cu elementele unui inel. Restul axiomelor pentru operația de adunare, ca şi pentru cea de înmulțire cu elementele inelului, rămân aceleaşi.

Definiție 4.2.6. *Fie R un inel unitar şi (M, +) un grup comutativ. Spunem că M este un R-modul la stânga, sau modul la stânga peste R, dacă este definită o operație externă*

$$\cdot : R\times M \to M,\ (a,x) \to ax$$

care satisface condițiile:

1. 1x=x, oricare ar fi $x\in M$.

2. (ab)x = a(bx) oricare ar fi $a,b\in R$ şi $x\in M$;

3. (a+b)x = ax + bx oricare ar fi $a,b\in R$ şi $x\in M$;

4. a(x + y) = ax + ay oricare ar fi $a\in R$ şi $x, y\in M$.

În mod analog se defineşte noțiunea duală de *R-modul la dreapta* (operație externă $\cdot$:M $\times$ R$\to$M) . Grupul comutativ (M, +) se numeşte *grupul aditiv subiacent* R-modulului. Elementele lui R se vor numi *scalari* iar operația externă *înmulțire cu scalari*. Faptul că M este un R-modul la stânga, respectiv la dreapta se mai notează prin $_RM$, respectiv M_R. În cele ce urmează, dacă nu menționăm contrariul, prin R-modul vom înțelege un R-modul la stânga, noțiunile şi rezultatele prezentate transpunându-se direct şi pentru R-module la dreapta.

Exemplul 4.2.7. *Un inel unitar R poate fi privit ca un R-modul la stânga, considerând grupul aditiv subiacent inelului R, împreună cu operația externă R$\times$ M $\to$ M, (a,x) $\to$ ax, unde ax este produsul (în R) al elementelor a şi x din inelul R.*

Exemplul 4.2.8. *Fie R un inel comutativ şi unitar şi n $\geq$ 1 un număr natural. Mulțimea*

$$R_n[X] = \{P \in R[X],\ grad(P) \leq n\}$$

este un R-modul dacă considerăm grupul aditiv subiacent determinat de adunarea obişnuită a polinoamelor, şi drept operaţie externă, înmulţirea polinoamelor cu elemente din R:

$$(a,\ a_0 + a_1X + \ldots + a_nX^n) \to aa_0 + aa_1X + \ldots + aa_nX^n.$$

Analog, mulţimea R[X] a tuturor polinoamelor cu coeficienţi în R poate fi înzestrată cu o structură de R modul.

Exemplul 4.2.9. *Fie R un inel comutativ şi unitar şi m şi n două numere naturale. Mulţimea $M_{m,n}(R)$ a matricelor cu m linii şi n coloane cu elemente din R poate fi înzestrată cu o structură de R-modul luând drept adunare adunarea obişnuită a matricelor, şi drept operaţie externă:*

$$(a,\ (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}) \to (aa_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}.$$

Propoziţia 4.2.10. *Fie M este un R-modul. Dacă a,b∈R şi x,y∈M, atunci:*

1. *a0 = 0x =0.*
2. *(-a)x = -ax, a(-x) = -ax, (-a)(-x) = ax.*
3. *a(x-y) = ax -ay.*
4. *(a - b)x = ax - bx.*
5. *Dacă, în plus, R este corp şi ax=0, atunci a=0 sau x=0.*

Demonstraţie. Se ţine seama de definiţia R-modului (vezi demonstraţia propoziţiei 1.2/pg. 244 [5]).

Definiția 4.2.11. *Fie M un R-modul la stânga. O submulțime $N \subset M$ se numeşte submodul al lui M dacă sunt îndeplinite următoarele condiții:*

1. *oricare ar fi $x, y \in N$, atunci $x-y \in N$.*
2. *oricare ar fi $a \in R$ şi $x \in M$, atunci $ax \in N$.*

Submodulul {0} se va numi submodulul nul al lui M.

Definiția 4.2.12. *Fie M un R-modul la stânga şi S o submulțime a lui M. Intersecția tuturor submodulelor la stânga ale lui R care conțin mulțimea S se numeşte submodulul generat de S şi se notează cu <S>. Se spune că S este un sistem de generatori pentru <S>. Submodulul generat de mulțimea vidă este submodulul nul. Submodulul $<\{x\}> = \{ax,\ a \in R\}$ se numeşte submodulul ciclic sau monogen al lui M generat de $x \in M$, şi se notează Rx sau <x>. Dacă M =Rx, atunci M se numeşte modul ciclic.*

Dacă $\{N_i\}_{i\in I}$ este o familie de submodule ale lui M, submodulul generat de $\bigcup_{i\in I} N_i$ se numeşte suma familiei de submodule $\{N_i\}_{i\in I}$ şi se notează $\sum_{i\in I} N_i$.

Se poate arăta că

$$<S> = \{ \sum_{i=1}^{n} a_i x_i ,\ a_i \in R,\ x_i \in S,\ n \in \mathbf{N}\}$$

Dacă $\{N_i\}_{i\in I}$ este o familie de submodule ale lui M, atunci

$$\sum_{i\in I} N_i = < \bigcup_{i\in I} N_i > = \{ \sum_{i=1}^{n} x_{j_i} ,\ x_{j_i} \in N_{j_i},\ j_i \in I,\ n \in \mathbf{N}\}$$

În particular, dacă N_1, N_2, …, N_p sunt submodule ale unui R-modul M, atunci

$$\sum_{i=1}^{p} N_i = \{\sum_{i=1}^{p} x_i \text{ , } x_i \in N_i\}$$

Dacă reprezentarea fiecărui element din $\sum_{i=1}^{p} N_i$ sub forma $\sum_{i=1}^{p} x_i$, cu $x_i \in N_i$ pentru orice i, este unică, atunci spunem că suma familiei de submodule este directă şi folosim scrierea $N_1 \oplus N_2 \oplus \ldots \oplus N_p$.

Definiția 4.2.13. *Fie M şi N două R-module. Se numeşte morfism de R-module de la M la N o funcție φ: M $\to$ N astfel încât să fie satisfăcute următoarele condiții:*

1. $\varphi(x+y) = \varphi(x) + \varphi(y)$ oricare ar fi x, y $\in$ M.

2. $\varphi(ax) = a\varphi(x)$ oricare ar fi $a \in R$ şi x $\in$ M.

Dacă, în plus, φ este o funcție bijectivă, atunci φ se numeşte izomorfism de R-module.

Dacă

$$\varphi : M \to N$$

este un morfism de R-module atunci

1. Ker φ = $\{x \in M: \varphi(x) = 0\}$ este un submodul al lui M numit *nucleul morfismului* φ.
2. Im φ = φ/M) = $\{\varphi(x), x \in M\}$ este un submodul al lui N numit *imaginea morfismului* φ.

Definiție 4.2.14. *Fie M un R- modul şi $N \subset M$ un submodul al său. Definim pe M următoarea relație de echivalență:*

$$x \sim y \text{ dacă şi numai dacă } x - y \in N.$$

Clasa de echivalență a lui $x \in N$ este $\overline{x} = \{x + z, z \in N\}$.

Fie $M/N = \{\overline{x}, x \in M\}$. *M/N are o structură de R-modul relativ la următoarele operații:*

adunare: $\overline{x} + \overline{y} = \overline{x + y}$ *oricare ar fi* $\overline{x}, \overline{y} \in M/N$.

înmulțire cu scalari din R: $a\overline{x} = \overline{ax}$ *oricare ar fi* $a \in R$ *şi* $\overline{x} \in M/N$.

Mulțimea M/N cu operațiile definite mai sus se numeşte modulul factor al lui M prin submodulul N. Nu este greu de observat că funcția surjectivă $\pi: M \to M/N$, $\pi(x) = \overline{x}$, *este un morfism de R-module, numit morfismul canonic de la M la M/N.*

Teorema 4.2.15. ***(Teorema fundamentală de izomorfism)*** *Fie $f: M \to N$ un morfism de R module. Atunci există un unic izomorfism de R-module*

$$\varphi : M/Ker\, f \to Im\, f$$

astfel încât $f = \varphi \circ \pi$, unde π este morfismul canonic de la M la M/Ker f.

Fie M un modul peste un inel unitar R. Noțiunile de sistem de generatori şi mulțime liniar independentă se definesc la fel ca în cazul spațiilor vectoriale. Elementul $x \in M$ este *combinație liniară* cu coeficienți în R a familiei de elemente $(x_i)_{i \in I}$ ale lui M, dacă x se poate scrie sub forma $x = \sum_{i \in I} a_i x_i$, unde numai un număr finit dintre coeficienții a_i sunt nenuli. Familia S = $(x_i)_{i\in I}$ de elemente din M este *sistem de generatori* pentru M dacă pentru orice $x \in M$ există familia finită $I_0 \subset I$ astfel încât $x = \sum_{i\in I_0} a_i x_i$. Un modul care admite o mulțime finită de generatori se numeşte modul *finit generat* sau de *tip finit*. Familia $(x_i)_{i\in I}$ de elemente din M este *liniar independentă* dacă 0 se poate scrie ca o combinație liniară (cu coeficienți în R) de elemente din familie dacă şi numai dacă toți scalarii sunt nuli. Mai precis, pentru orice familie finită $I_0 \subset I$ avem

$$\sum_{i\in I_0} a_i x_i = 0 \Leftrightarrow a_i = 0 \text{ oricare ar fi } i\in I_0 .$$

Evident orice submulțime a unei familii liniar independente este la rândul ei o familie liniar independentă.

Definiția 4.2.16. *O familie B de elemente ale unui R-modul M se numeşte bază dacă îndeplineşte condițiile de mai jos:*

a) B este liniar independentă;

b) B este sistem de generatori pentru M.

Un modul care admite o bază se numeşte modul liber. Dacă R este un inel comutativ spunem că un R-modul liber M are rang infinit dacă admite o bază infinită. Dacă M are o bază finită spunem că este de rang finit iar numărul de elemente al unei baze se numeşte rangul R-modulului M şi se notează cu $rang_R M$ (se poate arăta că $rang_R M$ nu depinde de baza aleasă pentru module libere M peste inele comutative R).

Teorema 4.2.17. *(teorema 3.4./pg. 257 [5]) Fie L un R-modul liber de bază $B = \{e_i\}_{i\in I}$. Atunci oricare ar fi R-modulul M şi* *oricare ar fi familia $\{x_i\}_{i\in I}$ de elemente din M, există un unic morfism de R-module $\varphi : L \to M$ astfel încât $\varphi(e_i) = x_i$ pentru orice $i \in I$. Mai mult, φ este injectivă (respectiv surjectivă, bijectivă) dacă şi numai dacă $\{x_i\}_{i\in I}$ este un sistem liniar independent (respectiv sistem de generatori, bază).*

Teorema 4.2.18. *(teorema 2.1./pg. 204 [5i]) Fie R un inel principal şi F un R-modul liber de rang n. Dacă L este un submodul al lui F, atunci:*

1. *L este liber de rang $m \le n$.*
2. *Există o bază $\{g_1, g_2, \ldots, g_m\}$ a lui R şi o bază $\{f_1, f_2, \ldots, f_n\}$ a lui F astfel încât*

$$g_i = d_i f_i,\ 1 \le i \le m$$

unde $d_i \in R$, $d_i \neq 0$, $1 \le i \le m$ şi $d_1 / d_2 / \ldots / d_m$.

Notația 4.2.19. Fie M un modul peste un inel principal R şi x un element din M. Se notează cu $\mathrm{Ann}_R(x)$ idealul

$$\mathrm{Ann}_R(x) = \{a \in R,\ ax = 0\}$$

Deoarece R este inel principal rezultă că există $\mu_x \in R$ astfel încât $\mathrm{Ann}_R(x) = R\mu_x$. Elementul $\mu_x \in R$ se numeşte *ordinul* lui $x \in M$ (μ_x este unic determinat mai puțin o asociere în divizibilitate). Dacă $R = K[X]$, K corp comutativ, μ_x este unic determinat dacă cere să fie polinom unitar. Elementul x se numeşte *element de torsiune (sau torsionat)* dacă $\mathrm{Ann}_R(x) \neq \{0\}$. Se notează cu t(M) mulțimea elementelor de torsiune din M. t(M) este un submodul numit submodulul de torsiune al lui M. Dacă t(M) = M, spunem că M este modul de torsiune, iar dacă t(M) = {0} spunem că M este modul fără torsiune. Evident, $t(M) = \{x \in M, \mu_x \neq 0\}$.

Funcția

$$f : R \to Rx,\ f(a) = ax \text{ oricare ar fi } a \in R$$

este un morfism surjectiv de R module al cărui nucleu Ker f = $Ann_R(x)$. Aplicând teorema fundamentală de izomorfism obținem

$$Rx \cong R/\mathrm{Ker}\ f = R/Ann_R(x) = R/R\mu_x.$$

Teorema 4.2.20. ***(Teorema factorilor invarianți)*** *Fie M un modul de tip finit peste un inel principal R. Atunci există două numere naturale m şi n, $m \le n$ şi elementele $x_1, x_2, \ldots, x_n \in M$ astfel încât*

1. $M = \underbrace{Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_m}_{t(M)} \oplus Rx_{m+1} \oplus \ldots \oplus Rx_n$

şi, în plus,

$$\begin{cases} \mu_{x_i} \neq 0\ \mu_{x_i} \notin U(R) \text{ pentru orice } 1 \le i \le m \\ \mu_{x_1} | \mu_{x_2} | \ldots | \mu_{x_m} \\ \mu_{x_i} = 0 \text{ pentru orice } m < i \le n. \end{cases}$$

2. *Numerele naturale m şi n precum şi elementele $d_i = \mu_{x_i} \in R$, $1 \le i \le m$ sunt unic determinate (până la o asociere în divizibilitate) (teorema 2.7/pg. 209 [5i]).*

Definiția 4.2.21. *Elementele* $d_i = \mu_{x_i}$ *$1 \leq i \leq m$ a căror existență este demonstrată în teorema precedentă se numesc factorii invarianți ai modulului M (sunt unici mai puțin o asociere în divizibilitate). Divizorii elementari ai modulului M reprezintă factorii ireductibili la puterea maximă la care apar în descompunerea fiecăruia dintre factorii invarianți.*

Teorema 4.2.22. *(lema 3.1/pg. 212 [4i])Fie M un modul peste un inel principal R şi $\mu_1, \mu_2, \ldots \mu_r \in R$ astfel încât $(\mu_i, \mu_j) = 1$ pentru orice $i \neq j$. Atunci*

1. Dacă $x \in M$ şi $\mu_x = \mu_1\mu_2 \ldots \mu_r$, atunci există $x_1, x_2, \ldots, x_r \in M$ astfel încât

$$\begin{cases} Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_r = Rx \\ \mu_{x_i} = \mu_i \text{ pentru orice } 1 \leq i \leq r. \end{cases}$$

2. Dacă $x_1, x_2, \ldots, x_r \in M$ au proprietatea că $\mu_{x_i} = \mu_i$ pentru orice $1 \leq i \leq r$, atunci există $x \in M$ astfel încât

$$\begin{cases} Rx = Rx_1 \oplus Rx_2 \oplus \ldots \oplus Rx_r \\ \mu_x = \mu_1\mu_2 \ldots \mu_r. \end{cases}$$

Definiția 4.2.23. *Un R-modul M nenul se numeşte indecompozabil dacă din $M = X \oplus Y$, unde X ş Y sunt submodule ale lui M, rezultă $X = \{0\}$ sau $X = M$.*

Teorema 4.2.24. *(teorema 3.3/pg. 212 [4])Dacă M este un modul indecompozabil de tip finit peste un inel principal R, atunci M este izomorf cu R, sau M este izomorf cu $R/R\pi^k$,* *unde π este un element ireductibil al lui R şi k un număr întreg pozitiv.*

Demonstrație. Dacă M este indecompozabil, atunci M =Rx, unde fie μ_x =0, fie $\mu_x \neq 0$. Dacă μ_x = 0, atunci M este izomorf cu R. Dacă $\mu_x \neq 0$, atunci μ_x de forma π^k (π ireductibil), altfel în descompunerea lui μ_x ar există factori ireductibili primi între ei, şi conform teoremei 4.2.22, M=Rx nu ar fi indecompozabil. În consecință, dacă $\mu_x \neq 0$, atunci M este izomorf cu $R/R\pi^k$, unde π este un element ireductibil al lui R şi k un număr întreg pozitiv.

Teorema 4.2.25. *(teorema 3.6/pg. 214 [4])Fie M un modul de tip finit peste un inel principal R şi*

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_p = N_1 \oplus N_2 \oplus ..N_q$$

două reprezentări ale lui M ca sumă directă de module indecompozabile. Atunci p = q şi există o permutare σ astfel încât $M_i = N_{\sigma(i)}$ pentru orice $1 \leq i \leq p$.

4.3. Polinomul minimal asociat unei transformări liniare

Fie K un corp comutativ şi V un spațiu vectorial peste K de dimensiune n. Fie u: V$\rightarrow$ V o transformare liniară şi A matricea asociată lui u într-o bază fixată B.

Fie K[X] inelul polinoamelor cu coeficienți în K (reamintim că acest inel este principal). Fie $M_{n,n}(K)$ inelul matricelor cu n linii şi n coloane cu elemente din K. Considerăm următoarele morfisme de inele

$$\eta : K[X] \rightarrow End_K(V)$$

$$\eta(P) = P(u) = \alpha_0 1_V + \alpha_1 u + \ldots + \alpha_s u^s,$$

pentru $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_s X^s$.

$$\xi : K[X] \to M_{n,n}(K)$$

$$\xi(P) = P(A) = \alpha_0 I_n + \alpha_1 A + \ldots + \alpha_s A^s,$$

pentru $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_s X^s$.

Deoarece K[X] este inel principal şi Ker η = Ker ξ sunt ideale în K[X] rezultă că există un polinom $\mu \in K[X]$ astfel încât

$$\text{Ker } \eta = \text{Ker } \xi = K[X]\mu.$$

Polinomul μ se numeşte *polinomul minimal* al transformării liniare u (respectiv al matricei A). Polinomul minimal este unic determinat de proprietățile:

1. este polinom unitar
2. $\mu(u) = 0$ (respectiv $\mu(A) = 0$)
3. dacă $P \in K[X]$ şi $P(u) = 0$ (respectiv $P(A) = 0$), atunci $\mu | P$.

Pe V definim o operație algebrică externă:

$$K[X] \times V \to V,\ (P, x) \to P \cdot x$$

$$P \cdot x = \eta(P)(x) = \alpha_0 x + \alpha_1 u(x) + \ldots + \alpha_s u^s(x),$$

pentru $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_s X^s$. V devine astfel un K[X]-modul la stânga (adunarea este dată de adunarea vectorilor din V).

Lema 4.3.1. *Fie L o submulțime a lui V. Următoarele afirmații sunt echivalente:*

1. *L este subspațiu invariant al lui u.*
2. *L este submodul al lui ${}_{K[X]}V$.*

Demonstrație. 1 => 2. Fie $P = \alpha_0 + \alpha_1 X + \ldots + a_s X^s \in K[X]$ şi $x \in V$. Avem $P \cdot x = \alpha_0 + \alpha_1 u(x) + \ldots + \alpha_s u^s(x) \in L$.

2 =>1 Evident dacă L este submodul în ${}_{K[X]}V$ atunci L este subspațiu vectorial al lui V. Pe de altă parte pentru orice $x\in L$, avem $u(x) = X\cdot x \in L$, şi deci L este invariant la u.

Lema 4.3.2. *Modulul ${}_{K[X]}V$ este finit generat şi t(V) = V.*

Demonstrație. Fie $B=\{e_1, e_2, \ldots, e_n\}$ baza fixată a lui a spațiului vectorial V peste K. Atunci

$$V = Ke_1 + Ke_2 + \ldots +Ke_n \subset K[X]e_1 + K[X]e_2 + \ldots +K[X]e_n \subset V.$$

Deci B este un sistem de generatori pentru ${}_{K[X]}V$.

Fie $x\in V$. Familia $\{x, u(x), \ldots, u^n(x)\}$ de elemente din spațiu vectorial n-dimensional V este liniar dependentă (are n+1 elemente). Ca urmare, există scalarii $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$, nu toți nuli, astfel încât

$$\alpha_0 x + \alpha_1 u(x) + \ldots +\alpha_n u^n(x) = 0$$

şi deci $P\cdot x = 0$ pentru $P = \alpha_0 + \alpha_1 X + \ldots +\alpha_n X^n$, $P \neq 0$. În consecință, $x\in t(V)$.

Lema 4.3.3. *Fie μ polinomul minimal al transformării liniare u.*

1. *Dacă $d_1/ d_2/\ldots/ d_m$ sunt factorii invarianți ai K[X]-modulului ${}_{K[X]}V$, atunci $\mu = d_m$.*
2. *Există $x \in V$ astfel încât $\mu = \mu_x$.*

Demonstrație. Dacă $d_1| d_2|\ldots| d_m$ sunt factorii invarianți ai K[X]-modulului ${}_{K[X]}V$, ținând seama că t(V) = V, rezultă că

$$V = K[X]x_1\oplus K[X]x_2\oplus\ldots\oplus K[X]x_m$$

unde $\mu_{x_i} = d_i$ pentru orice $1\leq i\leq m$ ($Ann_{K[X]}(x_i) = d_iK[X]$) . Deoarece $d_i|d_m$ pentru orice $1\leq i\leq m$, rezultă că există b_i astfel încât $d_m =b_id_i$, şi în consecință

$$d_m \cdot x_i = b_i d_i \cdot x_i = b_i \cdot (d_i \cdot x_i) = 0$$

pentru orice $1 \leq i \leq m$.

Verificăm faptul că d_m îndeplineşte condițiile care caracterizează un polinom minimal. Dacă

$$x \in V = K[X]x_1 \oplus K[X]x_2 \oplus \ldots \oplus K[X]x_m,$$

atunci există scalarii $a_1, a_2, \ldots a_m \in K[X]$ astfel încât $x = \sum_{i=1}^{m} a_i \cdot x_i$, şi deci

$$d_m(u)(x) = d_m(u)\left(\sum_{i=1}^{m} a_i \cdot x_i\right) = \sum_{i=1}^{m} d_m(u)(a_i \cdot x_i) = \sum_{i=1}^{m} d_m \cdot (a_i \cdot x_i)$$

$$= \sum_{i=1}^{m} a_i \cdot (d_m \cdot x_i) = 0$$

Fie a un polinom din K[X] astfel încât a(u) = 0. Din faptul că

$$a \cdot x_m = a(u)(x_m) = 0$$

rezultă că $a \in Ann_{K[X]}(x_m) = K[X]\, d_m$, de unde se obține că $d_m | a$.

Am demonstrat astfel că d_m este polinom minimal al transformării liniare u. Punctul 2 din lema se verifică pentru că $d_m = \mu_{x_m}$.

Pentru orice $x \in V$,

$$K[X] \cdot x = \{\, \alpha_0 x + \alpha_1 u(x) + \ldots + \alpha_s u^s(x),\ s \in \mathbf{N},\ \alpha_i \in K,\ 1 \leq i \leq s \}$$

poate fi privit ca un subspațiu vectorial al lui V peste K.

Lema 4.3.4. *Pentru orice $x \in V$ avem dimensiunea lui $K[X] \cdot x$ privit ca un subspațiu vectorial al lui V peste K este egală cu gradul polinomului μ_x.*

Demonstrație. Fie $t = \text{grad}(\mu_x)$. Arătăm că $B_x = \{x, u(x), \ldots u^{t-1}(x)\}$ este o bază a lui $K[X] \cdot x$ peste K. Pentru a arăta că B_x este liniar independentă să considerăm scalarii $\alpha_0, \alpha_2, \ldots, \alpha_{t-1} \in K$ astfel încât

$$\alpha_0 x + \alpha_1 u(x) + \ \dots + \alpha_{t-1} u^{t-1}(x) = 0.$$

Polinomul $P = \alpha_0 + \alpha_1 X + \ \dots + \alpha_{t-1} X^{t-1} \in K[X]$ are deci proprietatea că $P\cdot x = 0$, ceea ce este echivalent cu $P \in \mathrm{Ann}_{K[X]}(x) = K[x]\mu_x$, de unde rezultă că $\mu_x | P$. Se obține că $P = 0$, fiindcă altfel

$$t = \mathrm{grad}(\mu_x) \le \mathrm{grad}(P) \le t-1.$$

Pentru a arăta că B_x este sistem de generatori, luăm un element oarecare y din $K[X]\cdot x$, adică un element de forma $P\cdot x$ cu $P\in K[X]$. Din teorema împărțirii cu rest rezultă că există $q \in K[X]$ şi $r \in K[X]$ astfel încât

$$P = \mu_x q + r,\ \mathrm{grad}(r) < \mathrm{grad}(\mu_x).$$

Din faptul că $\mathrm{grad}(r) < \mathrm{grad}(\mu_x)$ deducem că r este de forma

$$r = \alpha_0 + \alpha_1 X + \ \dots + \alpha_s X^s \ \text{ cu } s < t.$$

Avem

$$\begin{aligned} y &= P\cdot x = (\mu_x q + r)\cdot x = (\mu_x q)\cdot x + r\cdot x = q\cdot(\mu_x\cdot x) + r\cdot x \\ &= r\cdot x = (\alpha_0 + \alpha_1 X + \ \dots + \alpha_s X^s)\cdot x \\ &= \alpha_0 x + \alpha_1 u(x) + \ \dots + \alpha_s u^s(x) \\ &= \alpha_0 x + \alpha_1 u(x) + \ \dots + \alpha_s u^s(x) + 0u^{s+1}(x) + \dots + 0\, u^{t-1}(x). \end{aligned}$$

de unde rezultă că y este în spațiu generat de B_x.

Definiția 4.3.5. *O transformare liniară $u \in End_K(V)$ se numeşte ciclică dacă ${}_{K[X]}V$ este modul ciclic, i.e. dacă există $x\in V$ astfel încât $V = K[X]\cdot x$.*

Lema 4.3.6. *O transformare liniară $u \in End_K(V)$ este ciclică dacă şi numai dacă gradul polinomului minimal al lui u este egal cu dimensiunea lui V peste K.*

Demonstrație. Dacă u este ciclică, adică dacă $V = K[X]\cdot x$, atunci dimensiunea lui V este egală cu gradul polinomului minimal al lui u, deoarece acesta este egal cu dimensiunea lui K[X]·x conform lemei precedente.

Reciproc, dacă gradul polinomului minimal al lui u este egal cu dimensiunea lui V peste K, atunci aplicând lema precedentă, rezultă că dimensiunea lui K[X]·x privit ca subspațiu vectorial al lui V este egală cu dimensiunea lui V. În consecință se obține V = K[X]·x.

Teorema 4.3.7. *Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u \in End_K(V)$. Următoarele afirmații sunt echivalente:*

1. *V este indecompozabil relativ la u*
2. *Există $x \in V$ astfel încât $V = K[X]\cdot x$. şi $\mu_x = \pi^k$, unde k este un număr natural nenul şi π este un polinom ireductibil în K[X].*

Demonstrație. Rezultă aplicând lemele precedente şi teoremele 4.2.20. 4.2.22, 4.2.24.

Teorema 4.3.8 *Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u \in End_K(V)$. Atunci V poate fi reprezentat ca o sumă directă de subspații indecompozabile relativ la u. Asemenea descompuneri sunt unice, mai puțin un izomorfism de perechi (de K[X] - module) ale sumanzilor.*

Demonstrație. Se aplică teoremele 4.2.20 şi 4.2.25.

Definiția 4.3.9. *Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u \in End_K(V)$.Factorii invarianți (respectiv divizorii elementari) ai K[X]-modulului asociat* *lui u se numesc factori invarianți (respectiv divizori elementari) ai lui u. Factorii invarianți (respectiv divizorii elementari) ai lui u sunt unic determinați dacă impunem condiția să fie polinoame unitare.*

4.4. Matricea canonică Jordan a unei transformări liniare

Definiție 4.4.1. *Fie K un corp comutativ şi K[X] inelul polinoamelor cu coeficienți în K. Fie* $\pi = X^s - \alpha_{s-1}X^{s-1} - \dots - \alpha_1 X - \alpha_0$ *un polinom unitar din K[X]. Matricea* $C_\pi \in M_{s,s}(K)$

$$C_\pi = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & \dots & 0 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{s-2} & \alpha_{s-1} \end{pmatrix}$$

se numeşte companionul matriceal al polinomului π.

Dacă $P = \pi^k$, *unde k este un număr natural nenul, atunci definim matricea* $J_{\pi^k} \in M_{sk,sk}(K)$

$$J_{\pi^k} = \begin{pmatrix} C_\pi & N & & & 0 \\ & C_\pi & N & & \\ & & \ddots & \ddots & \\ & 0 & & C_\pi & N \\ & & & & C_\pi \end{pmatrix}$$

unde matricea $N \in M_{s,s}(K)$ *este*

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

Dacă π este un polinom ireductibil peste K (deci un element ireductibil în K[X]) şi k este un număr natural nenul atunci matricea J_{π^k} se numeşte celulă Jordan (peste K) asociată polinomului π^k.

O matrice de forma

$$\begin{pmatrix} J_{\pi_1^{k_1}} & & & 0 \\ & J_{\pi_2^{k_2}} & & \\ & & \ddots & \\ 0 & & & J_{\pi_p^{k_p}} \end{pmatrix}$$

unde π_1, π_2, …π_p sunt polinoame ireductibile peste K se numeşte matrice canonică Jordan peste K.

Definiția 4.4.2. *Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u \in End_K(V)$. Dacă $\pi_1^{k_1}, \pi_2^{k_2}$, …, $\pi_p^{k_p}$ sunt divizorii elementari ai transformării liniare u, atunci matricea J_u*

$$J_u = \begin{pmatrix} J_{\pi_1^{k_1}} & & & 0 \\ & J_{\pi_2^{k_2}} & & \\ & & \ddots & \\ 0 & & & J_{\pi_p^{k_p}} \end{pmatrix}$$

se numeşte matricea canonică Jordan a transformării liniare u.

Propoziția 4.4.3. *Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u\in End_K(V)$ o transformare liniară ciclică al cărei polinom minimal este de forma π^k, cu $\pi = X^s + \alpha_{s-1}X^{s-1} + \dots + \alpha_1 X + \alpha_0$ şi $k \geq 1$. Atunci există o bază $B = \{e_1, e_2, \dots, e_n\}$ a lui V astfel încât matricea asociată lui u în baza B să fie* J_{π^k} .

Demonstrație. Fie n dimensiunea lui V peste K. Deoarece u este transformare liniară ciclică, rezultă că există $x\in V$ astfel încât $V = K[X]\cdot x$, şi dimensiunea lui V peste K este egală cu gradul polinomului minimal al lui u (care este egal cu $\mu_x = \pi^k$). În consecință, n =sk. Definim următorii vectori din V:

$$e_1 = x,\ e_2 = X\cdot x,\ \dots,\ e_s = X^{s-1}\cdot x$$

$$e_{s+1} = \pi\cdot x,\ e_2 = (X\pi)\cdot x,\ \dots,\ e_s = (X^{s-1}\pi)\cdot x$$

$$\vdots$$

$$e_{(k-1)s+1} = \pi^{k-1}\cdot x,\ e_{(k-1)s+2} = (X\pi^{k-1})\cdot x,\ \dots,\ e_{ks} = (X^{s-1}\pi^{k-1})\cdot x$$

Observăm că fiecare e_i poate fi scris sub forma $e_i = P_i\cdot x$ cu $P_i\in K[X]$ având proprietatea că $grad(P_i) \leq s-1 +s(k-1) = sk -1 =n-1<n$. Mai mult, $grad(P_i) \neq grad(P_j)$ pentru orice $i\neq j$. Demonstrăm că $B = \{e_1, e_2, \dots, e_n\}$ este o bază a lui V peste K. Pentru această este suficient să arătăm că B este liniar independentă (deoarece numărul de vectori din B este egal cu dimensiunea spațiului vectorial V). Presupunem prin absurd că există scalarii $\beta_1, \beta_2, \dots, \beta_n \in K$, nu toți nuli, astfel încât

$$\beta_1 e_1 + \beta_2 e_2 + \dots + \beta_n e_n =0.$$

Ținând cont de definiția vectorilor din B, obținem

$$\beta_1(P_1\cdot x) + \beta_2(P_2\cdot x) + \dots + \beta_n(P_n\cdot x) =0 \iff$$

$$(\beta_1 P_1)\cdot x + (\beta_2 P_2)\cdot x + \dots + (\beta_n P_n)\cdot x =0 \iff$$

$(\beta_1P_1 + \beta_2P_2 + \ \ldots + \beta_nP_n)\cdot x = 0.$

Dacă notăm $P = \beta_1P_1 + \beta_2P_2 + \ \ldots + \beta_nP_n$, atunci

$$P \in \mathrm{Ann}_{K[X]}(x) = K[X]\mu_x = K[X]\pi^k.$$

De aici rezultă că $\pi^k \mid P$ şi deci

$$n = ks = \mathrm{grad}(\pi^k) \le \mathrm{grad}(P) \le \max\{\mathrm{grad}(P_i),\ 1 \le i \le n\} < n.$$

Am obținut o contradicție. Deci presupunerea că nu toți scalarii $\beta_1, \beta_2, \ldots, \beta_n \in K$ sunt nuli este falsă.

Vom arăta în continuare că matricea asociată lui u în bază B este J_{π^k}. Pentru aceasta este suficient să observăm că

$$u(e_1) = u(x) = X\cdot x = e_1$$

$$u(e_2) = u(X.x) = u(u(x)) = u^2(x) = X^2\cdot x = e_3$$

....

$$u(e_{s-1}) = u(X^{s-2}.x) = u(u^{s-2}(x)) = u^{s-1}(x) = X^{s-1}\cdot x = e_s$$

$$\begin{aligned}
u(e_s) &= u(X^{s-1}.x) = u(u^{s-1}(x)) = u^s(x) = X^s\cdot x = \pi\cdot x + (X^s - \pi)\cdot x \\
&= e_{s+1} + (-\alpha_{s-1}X^{s-1} - \ldots - \alpha_1X - \alpha_0)\cdot x \\
&= e_{s+1} - \alpha_{s-1}X^{s-1}\cdot x - \ldots - \alpha_1X\cdot x - \alpha_0\cdot x \\
&= e_{s+1} - \alpha_{s-1}e_s - \ldots - \alpha_1e_2 - \alpha_0\cdot e_1
\end{aligned}$$

$$\begin{aligned}
u(e_{s+1}) &= u(\pi\cdot x) \\
&= u(u^s(x) + \alpha_{s-1}u^{s-1}(x) + \ldots + \alpha_1u(x) + \alpha_0x) \\
&= u^{s+1}(x) + \alpha_{s-1}u^s(x) + \ldots + \alpha_1u^2(x) + \alpha_0u(x) = (X\pi)\cdot x \\
&= e_{s+2}
\end{aligned}$$

....

$$\begin{aligned}
u(e_{2s-1}) &= u(X^{s-2}\pi.x) \\
&= u(u^{2s-2}(x) + \alpha_{s-1}u^{2s-3}(x) + \ldots + \alpha_1u^{s-1}(x) + \alpha_0u^{s-2}(x)) \\
&= u^{2s-1}(x) + \alpha_{s-1}u^{2s-2}(x) + \ldots + \alpha_1u^s(x) + \alpha_0u^{s-1}(x) = (X^{s-1}\pi)\cdot x \\
&= e_{2s}
\end{aligned}$$

$$u(e_{2s}) = u(X^{s-1}\pi.x) = X\cdot(X^{s-1}\pi.x) = (X^s\pi)\cdot x = \pi^2\cdot x + (X^s - \pi)\pi\cdot x$$

$= e_{2s+1} + (-\alpha_{s-1}X^{s-1} - \ldots - \alpha_1 X - \alpha_0)\pi\cdot x$

$= e_{2s+1} - \alpha_{s-1}e_{2s} - \ldots - \alpha_1 e_{s+2} - \alpha_0\cdot e_{s+1}$

…

$u(e_n) = -\alpha_{s-1}e_n - \ldots - \alpha_1 e_{n-s+2} - \alpha_0\cdot e_{n-s+1}$

Teorema 4.4.4. *Fie V un spaţiu vectorial de dimensiune finită peste corpul comutativ K şi fie $u\in End_K(V)$ o transformare liniară. Atunci există o bază $B = \{e_1, e_2, \ldots, e_n\}$ a lui V astfel încât matricea asociată lui u în baza B să fie J_u.*

Demonstraţie. Fie $\pi_1^{k_1}, \pi_2^{k_2}, \ldots, \pi_p^{k_p}$ divizorii elementari ai transformării liniare u. Atunci există $x_1, x_2, \ldots, x_p \in V$ astfel încât

$$V = K[X]x_1 \oplus K[X]x_2 \oplus \ldots \oplus K[X]x_p$$

şi $\mu_{x_i} = \pi_i^{k_i}$ pentru orice $1\le i\le p$. Fie $L_i = K[X]\cdot x_i$, u_i aplicaţia liniară indusă de u pe L_i şi μ_i polinomul minimal al lui $u_i\in End_K(L_i)$. Atunci $\mu_i = \mu_{x_i} = \pi_i^{k_i}$ şi u_i este o transformare liniară ciclică. Din propoziţia precedentă rezultă că există o bază B_i în L_i astfel încât matricea $M_{B_i}(u_i)$ asociată lui u_i în baza B_i să fie $J_{\pi_i^{k_i}}$ pentru orice $1 \le i \le p$. Atunci matricea lui u în baza $B = \bigcup_{i=1}^{p} B_i$ este

$$M_B(u) = \begin{pmatrix} M_{B_1}(u_1) & & & \\ & M_{B_2}(u_2) & & \bigcirc \\ & & \ddots & \\ \bigcirc & & & M_{B_p}(u_p) \end{pmatrix}$$

$$= \begin{pmatrix} J_{\pi_1^{k_1}} & & & \\ & J_{\pi_2^{k_2}} & & \bigcirc \\ & & \ddots & \\ \bigcirc & & & J_{\pi_p^{k_p}} \end{pmatrix}$$

Celule Jordan în cazul în care K =R sau K= C

Cazul K = **C** (corpul numerelor complexe)

Deoarece **C** este un corp algebric închis, orice polinom unitar $\pi \in \mathbf{C}[X]$ este ireductibil dacă şi numai dacă este de forma $\pi = X - \alpha$ cu $\alpha \in \mathbf{C}$. Aşadar celula Jordan asociată polinomului π^k, $k \geq 1$ este

$$J_{(X-\alpha)^k} = \begin{pmatrix} \alpha & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

Cazul K = **R** (corpul numerelor reale)

Dacă $\pi \in \mathbf{R}[X]$ este un polinom unitar şi ireductibil (peste **R**) atunci π este fie de forma $\pi = X - \alpha$ cu $\alpha \in \mathbf{R}$, fie de forma $\pi = X^2 - \beta X - \gamma$ cu $\beta, \gamma \in \mathbf{R}$ şi $\beta^2 + 4\gamma < 0$.

Dacă $\pi = X - \alpha$ atunci companionul matriceal al polinomului π este $C_{(X-\alpha)} = (\alpha)$, iar celula Jordan asociată polinomului π^k, $k \geq 1$ este

$$J_{(X-\alpha)^k} = \begin{pmatrix} \alpha & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

Dacă $\pi = \pi = X^2 - \beta X - \gamma$ ($\beta,\gamma \in \mathbf{R}$ şi $\beta^2 + 4\gamma < 0$), atunci companionul matriceal al polinomului π este

$$C_{X^2-\beta X-\gamma} = \begin{pmatrix} 0 & 1 \\ \gamma & \beta \end{pmatrix}$$

iar celula Jordan asociată polinomului π^k, $k \geq 1$ este

$$J_{(X^2-\beta X-\gamma)^k} = \begin{pmatrix} \begin{matrix} 0 & 1 \\ \gamma & \beta \end{matrix} & \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix} & & & O \\ & \begin{matrix} 0 & 1 \\ \gamma & \beta \end{matrix} & \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix} & & \\ & & \begin{matrix} 0 & 1 \\ \gamma & \beta \end{matrix} & \ddots & \\ & & & \ddots & \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix} \\ & O & & & \begin{matrix} 0 & 1 \\ \gamma & \beta \end{matrix} \end{pmatrix}$$

4.5. Forma diagonal canonică a unei matrice

Definiția 4.5.1. *Fie R un inel principal. Două matrice $A,B \in M_{m,n}(R)$ se numesc aritmetic echivalente dacă există două matrice inversabile $U \in M_{m,m}(R)$ şi $V \in M_{n,n}(R)$ astfel încât*

$$A = UBV.$$

Două matrice $A,B \in M_{n,n}(R)$ se numesc asemenea dacă există o matrice inversabilă $P \in M_{n,n}(R)$ astfel încât

$$A = P^{-1}BP.$$

Matricele care reprezintă aceeaşi transformare liniară (între spaţii vectoriale de dimensiune finită) în perechi de baze diferite sunt matrice aritmetic echivalente. Matricele corespunzătoare aceluiaşi endomorfism în baze diferite sunt matrice asemenea (vezi teorema 4.3.7 şi corolarul 4.3.8) .

Definiţia 4.5.2. *Fie R un inel principal. Matricea* $A \in M_{m,n}(R)$ *are forma diagonal canonică dacă*

$$A = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & 0 & \\ & & \ddots & & & \\ & & & d_r & & \\ & 0 & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

unde $r \leq \min(m,n)$ *şi* $d_1/d_2/\ldots/d_r \neq 0$.

Vom arăta că orice matrice A este aritmetic echivalentă cu o matrice D sub formă diagonal canonică. Pentru aceasta este necesară noţiunea de transformare elementară.

Notaţii 4.5.2. *Fie R un inel comutativ şi* $M_{n,n}(R)$ *inelul matricelor pătrate n-dimensionale cu elemente din R. Pentru orice* $1 \leq i, j \leq n$ *notăm*

$$E_{ij} = \begin{array}{cc} \begin{array}{ccc} & j & \end{array} & \\ \begin{pmatrix} 0 & \vdots & 0 \\ & 1 & \cdots \\ 0 & & 0 \end{pmatrix} & \begin{array}{c} \\ i \\ \\ \end{array} \end{array}$$

Pentru orice $1 \leq i, j \leq n$, $i \neq j$ *şi orice* $a \in R$ *notăm*

$$T_{ij}(a)=\begin{array}{c c}
\begin{array}{ccc} & j & \end{array} & \\
\begin{pmatrix}
1 & & & 0 \\
 & 1 & & \\
 & & \ddots \quad a & \\
0 & & & 1
\end{pmatrix} & \begin{array}{c} \\ \\ i \\ \\ \end{array}
\end{array}$$

Pentru orice $1\leq i\leq n$ şi orice $a\in U(R)$ notăm

$$D_i(a) = \begin{array}{c c}
\begin{array}{ccc} & i & \end{array} & \\
\begin{pmatrix}
1 & & & & 0 \\
 & \ddots & & & \\
 & & 1 & & \\
 & & & a & & \\
 & & & & 1 & \\
 & & & & & \ddots \\
0 & & & & & & 1
\end{pmatrix} & \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \end{array}
\end{array}$$

Pentru orice $1\leq i<j\leq n$ notăm

$$P_{ij}=\begin{array}{c c}
\begin{array}{ccc} & i & \quad i \end{array} & \\
\begin{pmatrix}
1 & & & & & & & & \\
 & \ddots & & & & & & & \\
 & & 1 & & & & & & \\
 & & & 0 & & & 1 & & \\
 & & & & 1 & & & & \\
 & & & & & \ddots & & & \\
 & & & & & & 1 & & \\
 & & & 1 & & & 0 & & \\
 & & & & & & & 1 & \\
 & & & & & & & & \ddots \\
 & & & & & & & & & 1
\end{pmatrix} & \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \\ \end{array}
\end{array}$$

Ținând cont de notațiile precedente, se observă uşor că

1. $E_{ij}E_{st} =\delta_{js}E_{it}$
2. $T_{ij} =I_n + aE_{ij}$
3. $T_{ij}(0) = I_n$
4. $T_{ij}(a)\, T_{ij}(b) = T_{ij}(a+b)$

5. $T_{ij}(-a) = T_{ij}(a)^{-1}$
6. $\det(T_{ij}(a)) = 1$
7. $D_i(1) = I_n$
8. $D_i(a)\, D_i(b) = D_i(ab)$
9. $D_i(a^{-1}) = D_i(a)^{-1}$
10. $\det(D_i(a)) = a$
11. $P_{ij}P_{ij} = I_n$ $(P_{ij} = P_{ij}^{-1})$

Dacă $A \in M_{m,n}(R)$, atunci matricea

- $AT_{ij}(a)$ se obține din A adunând la coloana j coloana i înmulțită cu a
- $AD_i(a)$ se obține din A înmulțind elementele coloanei i cu a
- AP_{ij} se obține din A permutând coloana i cu coloana j

Dacă $A \in M_{n,m}(R)$, atunci matricea

- $T_{ij}(a)A$ se obține din A adunând la linia i linia j înmulțită cu a
- $D_i(a)A$ se obține din A înmulțind elementele liniei i cu a
- $P_{ij}A$ se obține din A permutând linia i cu linia j

Se poate arăta că dacă R este un inel euclidian, atunci orice matrice din $M_{n,n}(R)$ al cărei determinant este 1 se poate scrie ca un produs finit de matrice de forma $T_{ij}(a)$, $a \in R$. De asemenea, dacă R este un inel euclidian, atunci orice matrice inversabilă A din $M_{n,n}(R)$ este egală cu un produs finit de matrice de forma $T_{ij}(a)$ şi o matrice de forma $D_i(a)$ (unde $a = \det(A)$). Matricele de forma $T_{ij}(a)$, $D_i(a)$ şi P_{ij} se numesc *matrice elementare*, iar transformările liniare care le corespund se numesc transformări elementare.

Teorema 4.5.4. *Fie R un inel principal şi A o matrice din $M_{m,n}(R)$. Atunci există o matrice D sub forma diagonal canonică astfel încât A ~ D (A este aritmetic echivalentă cu D).*

Demonstrație. Vom schița o demonstrație constructivă. Trecerea de la A la D se va face prin transformări succesive. Sunt posibile două cazuri:

1. există un element a_{ij} al matricei care divide toate elementele matricei
2. ar fi i şi j există elemente ale matricei A care nu se divid cu a_{ij}.

    2.a. există i şi j şi există pe linia i sau coloana j elemente care nu se divid cu a_{ij}.

    2.b. există un element a_{ij} al matricei care divide toate elementele de pe linia i şi coloana j (dar nu divide toate elementele matricei A)

Dacă ne plasăm în cazul 1, prin permutarea liniei i cu linia 1 şi coloanei j cu coloana 1, elementul a_{ij} ajunge în locul lui a_{11}. Deoarece (noul) $a_{11}| a_{1k}$, rezultă că există d_k astfel încât $a_{1k} = a_{11}d_k$. Deci înmulțind coloana 1 cu $-d_k$ şi adunând-o la coloana k elementul pe poziția (1,k) devine 0. Deci prin înmulțirea succesivă la dreapta a matricei A cu matrice $T_{1k}(-d_k)$ $(k \geq 2)$ elementele de pe prima linie, mai puțin a_{11}, devin 0. Similar, $a_{11}| a_{k1}$, deci există c_k astfel încât $a_{k1} = a_{11}c_k$. Deci înmulțind linia 1 cu $-c_k$ şi adunând-o la linia k elementul pe poziția (k, 1) devine 0. Deci prin înmulțirea succesivă la stânga a matricei A cu matrice $T_{k1}(-c_k)$ $(k \geq 2)$ elementele de pe prima coloană, mai puțin a_{11}, devin 0. După acesta se continuă diagonalizarea cu submatricea formată din ultimele m-1 linii şi n-1 coloane.

Dacă ne plasăm în cazul 2.a, considerăm un element $a_{ij} \neq 0$ cu proprietatea că numărul de factori primi din descompunerea lui este cel mai mic, şi permutăm linia i cu linia 1 şi coloana j cu coloana 1. Atunci fie pe prima linie fie pe prima coloană există un element care nu se divide cu a_{11}. Dacă a_{1k} este un element de pe prima linie care nu se divide cu a_{11}, permutăm coloana k cu coloana 2 şi considerăm că $d \in R$ este cel mai mare divizor comun al lui a_{12} şi a_{11}. Atunci există u, v, a, b $\in R$ astfel încât

$$d = ua_{11} + va_{12},\ a_{11} = da,\ a_{12} = db.$$

Matricea

$$V = \begin{pmatrix} u & -b & & & \\ v & a & & & 0 \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

are determinantul egal cu 1, deci este inversabilă. Matricea AV se obține din matricea A prin înlocuirea primelor 2 coloane, după cum urmează

$C_1 \leftarrow uC_1 + vC_2$

$C_2 \leftarrow (-b)C_1 + aC_2$

Elementul de pe poziția (1,1) al matricei AV este d. Numărul de factori primi din descompunerea lui d este strict mai mic decât numărul de factori primi din descompunerea lui a_{11}. Se continuă algoritmul cu noua matrice AV. Se procedează similar în cazul în care elementul care nu se divide cu a_{11} se află pe prima coloană.

Dacă ne plasăm în cazul 2.b, procedând ca în cazul 1 obținem o matrice aritmetic echivalentă cu A ale cărei elemente de pe prima linie şi prima coloană, cu excepția lui a_{11}, sunt egale cu zero. Dacă a_{pq} este un element din noua matrice care nu se divide cu a_{11}, atunci adunăm la linia p linia 1 (sau la coloana q coloana 1). Matricea obținută în urma acestei transformări satisface condițiile corespunzătoare cazului 2.a. În toate cele trei cazuri s-a redus problema la matrice A' aritmetic echivalentă cu A, fie cu număr de linii şi coloane mai mic decât pentru A, fie având proprietatea că $l(A') \leq l(A)$,unde

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

$l(a_{ij})$ = numărul de factori primi din descompunerea lui a_{ij}.

Formal demonstrația acestei teoreme se face prin inducție după dimensiunea (m,n) a matricei A şi l(A).

Observația 4.4.5. Dacă (R, φ) este inel euclidian (φ fiind funcția ce intervine în definiția acestuia), atunci în demonstrația teoremei anterioare putem face inducția după dimensiunea (m,n) a matricei A şi

$$\varphi(A) = \min\{\varphi(a_{ij}),\ a_{ij} \neq 0,\ 1 \le i \le m,\ 1 \le j \le n\}.$$

De asemenea matricea V utilizată în cazul 2.a poate fi înlocuită cu matricea elementară $T_{12}(-q)$, unde

$$a_{12} = a_{11}q + r,\ \varphi(r) < \varphi(a_{11}).$$

Deci în cazul unui inel euclidian putem găsi o matrice diagonal-canonică D aritmetic echivalentă cu A prin aplicarea unui număr finit de transformări elementare.

Observație 4.4.6. Calculele pentru obținerea matricei diagonal canonice D a unei matrice A pot fi organizate astfel încât să se obțină şi matricele U şi V (D =UAV):

$$\left(\begin{array}{c|c} A & I_m \\ \hline I_n & \end{array}\right) \to \left(\begin{array}{c|c} U_0AV_0 & U_0 \\ \hline V_0 & \end{array}\right) \to \ldots \left(\begin{array}{c|c} UAV & U \\ \hline V & \end{array}\right)$$

Exemplul 4.5.7. *Fie matricea din $M_{2,3}(\mathbf{Z})$:*

$$A = \begin{pmatrix} 3 & 4 & 6 \\ 2 & 6 & -4 \end{pmatrix}$$

$$\left(\begin{array}{ccc|cc} 3 & 4 & 6 & 1 & 0 \\ 2 & 6 & -4 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \underset{\substack{1 = (-1)3 + 1\cdot 4 \\ C_1 \leftarrow (-1)C_1 + C_2 \\ C_2 \leftarrow (-4)C_1 + 3C_2}}{\longrightarrow} \left(\begin{array}{ccc|cc} 1 & 0 & 6 & 1 & 0 \\ 4 & 10 & -4 & 0 & 1 \\ \hline -1 & -4 & 0 & & \\ 1 & 3 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)$$

$$\underset{C_3 \leftarrow C_3 - 6C_1}{\longrightarrow} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 4 & 10 & -28 & 0 & 1 \\ \hline -1 & -4 & 6 & & \\ 1 & 3 & -6 & & \\ 0 & 0 & 1 & & \end{array}\right) \underset{L_2 \leftarrow L_2 - 4L_1}{\longrightarrow}$$

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 10 & -28 & -4 & 1 \\ \hline -1 & -4 & 6 & & \\ 1 & 3 & -6 & & \\ 0 & 0 & 1 & & \end{array}\right) \underset{\substack{2 = 3\cdot 10 + 1\cdot(-28) \\ C_2 \leftarrow 3C_2 + C_3 \\ C_3 \leftarrow 14C_2 + 5C_3}}{\longrightarrow} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & -4 & 1 \\ \hline -1 & -6 & -26 & & \\ 1 & 3 & 12 & & \\ 0 & 1 & 5 & & \end{array}\right)$$

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \quad U = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \quad V = \begin{pmatrix} -1 & -6 & -26 \\ 1 & 3 & 12 \\ 0 & 1 & 5 \end{pmatrix}$$

Se verifică faptul că $UAV = D$.

Ținând cont că $\mathbf{Z}$ *este inel euclidian, putem obține forma canonică a lui A aplicând doar transformări elementare, după cum urmează:*

$$\left(\begin{array}{ccc|cc} 3 & 4 & 6 & 1 & 0 \\ 2 & 6 & -4 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \underset{L_1 \leftrightarrow L_2}{\longrightarrow} \left(\begin{array}{ccc|cc} 2 & 6 & -4 & 0 & 1 \\ 3 & 4 & 6 & 1 & 0 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)$$

$$\xrightarrow[\substack{3=2\cdot 1+1\\ L_2\leftarrow L_2-L_1}]{}\left(\begin{array}{ccc|cc} 2 & 6 & -4 & 0 & 1\\ 1 & -2 & 10 & 1 & -1\\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)\xrightarrow[L_1\leftrightarrow L_2]{}$$

$$\left(\begin{array}{ccc|cc} 1 & -2 & 10 & 1 & -1\\ 2 & 6 & -4 & 0 & 1\\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)\xrightarrow[L_2\leftarrow L_2-2L_1]{}\left(\begin{array}{ccc|cc} 1 & -2 & 10 & 1 & -1\\ 0 & 10 & -24 & -2 & 3\\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)$$

$$\xrightarrow[\substack{C_2\leftarrow C_2+2C_1\\ C_3\leftarrow C_3-10C_1}]{}\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 10 & -24 & -2 & 3\\ \hline 1 & 2 & -10 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)\xrightarrow[\substack{-24=10(-3)+6\\ C_3\leftarrow C_3+3C_2}]{}$$

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 10 & 6 & -2 & 3\\ \hline 1 & 2 & -4 & & \\ 0 & 1 & 3 & & \\ 0 & 0 & 1 & & \end{array}\right)\xrightarrow[\substack{10=6\cdot 1+4\\ C_2\leftarrow C_2-C_3}]{}\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 4 & 6 & -2 & 3\\ \hline 1 & 6 & -4 & & \\ 0 & -2 & 3 & & \\ 0 & -1 & 1 & & \end{array}\right)$$

$$\xrightarrow[\substack{6=4\cdot 1+2\\ C_3\leftarrow C_3-C_2}]{}\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 4 & 2 & -2 & 3\\ \hline 1 & 6 & -10 & & \\ 0 & -2 & 5 & & \\ 0 & -1 & 2 & & \end{array}\right)\xrightarrow[C_2\leftrightarrow C_3]{}$$

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 2 & 4 & -2 & 3\\ \hline 1 & -10 & 6 & & \\ 0 & 5 & -2 & & \\ 0 & 2 & -1 & & \end{array}\right)\xrightarrow[C_3\leftarrow C_3-2C_2]{}\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & -1\\ 0 & 2 & 0 & -2 & 3\\ \hline 1 & -10 & 26 & & \\ 0 & 5 & -12 & & \\ 0 & 2 & -5 & & \end{array}\right)$$

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \quad U = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \quad V = \begin{pmatrix} 1 & -10 & 26 \\ 0 & 5 & -12 \\ 0 & 2 & -5 \end{pmatrix}$$

Se verifică faptul că $UAV = D$.

Observația 4.5.8. Fie R un inel principal. Pentru orice matrice $A \in M_{m,n}(R)$ notăm cu $\Delta_k(A)$ cel mai mare divizor comun al minorilor de ordin k ai lui A ($1 \leq k \leq \min(m,n)$). De asemenea dacă $a,b \in R$ şi $a|\, b$, atunci notăm b/a acel element $c \in R$ astfel încât $b = ca$. Dacă $A,B \in M_{m,n}(R)$ sunt două matrice aritmetic echivalente, atunci $\Delta_k(A)$ şi $\Delta_k(B)$ sunt două elemente ale inelului R asociate în divizibilitate pentru orice $1 \leq k \leq \min(m,n)$. (Într-adevăr, dacă pentru o matrice A notăm cu C_j^A, respectiv L_j^A, coloana j, respectiv linia j a matricei A, atunci

$$C_j^{AV} = v_{1j}C_1^A + v_{2j}C_2^A + \ldots + v_{nj}C_n^A$$

$$L_j^{UA} = u_{j1}L_1^A + u_{j2}L_2^A + \ldots + u_{jn}L_n^A.$$

Ca urmare $\Delta_k(A)|\Delta_k(AV)$ şi $\Delta_k(A)|\Delta_k(AV)$ pentru orice k. Deoarece $A,B \in M_{m,n}(R)$ sunt aritmetic echivalente, există două matrice inversabile $U \in M_{m,m}(R)$ şi $V \in M_{n,n}(R)$ astfel încât $UAV = B$. Atunci $\Delta_k(A)|\Delta_k(AV)$ $\Delta_k(U(AV)) = \Delta_k(B)$. Cum $U^{-1}BV^{-1} = A$, avem şi $\Delta_k(B)|\Delta_k(A)$, de unde $\Delta_k(A) \sim \Delta_k(B)$)

Fie D o matrice sub formă diagonal canonică aritmetic echivalentă cu A :

$$\begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

Avem $\Delta_1(D) = d_1$, $\Delta_2(D) = d_1 d_2$ …, $\Delta_r = d_1\, d_2 \dots d_r$, $\Delta_j(D) = 0$ pentru orice $j \geq r+1$.

Datorită faptului că A şi D sunt aritmetic echivalente

$d_1 \sim \Delta_1(A)$ (asociere în divizibilitate),

$d_2 \sim \Delta_2(A)/\, d_1 \sim \Delta_2(A)/\, \Delta_1(A)$ (deoarece $\Delta_2(A) \sim d_1 d_2$)

....

$d_r \sim \Delta_r(A)/\, d_1 d_2 .. d_{r-1} \sim \Delta_r(A)/\, \Delta_{r-1}(A)$

$d_j = 0 \iff \Delta_j(A) = 0$ ($j \geq r+1$).

În concluzie matricea sub formă diagonal canonică D cu care A este aritmetic echivalentă este unic determinată mai puţin o asociere în divizibilitate a elementelor de pe diagonală. Convenim să numim matricea D *formă diagonal canonică* a matricei A.

Fie

$$A = \begin{pmatrix} 3 & 4 & 6 \\ 2 & 6 & -4 \end{pmatrix}$$

matricea din exemplul 4.5.7. Atunci $\Delta_1(A) = 1$ (sau $-1 \sim 1$). Minorii de ordinul 2 ai lui A sunt

$$\begin{vmatrix} 3 & 4 \\ 2 & 6 \end{vmatrix} = 10 \qquad \begin{vmatrix} 3 & 6 \\ 2 & -4 \end{vmatrix} = -24 \qquad \begin{vmatrix} 4 & 6 \\ 6 & -4 \end{vmatrix} = -52.$$

Deci $\Delta_2(A) = 2$ (sau $-2 \sim 2$). În consecinţă putem scrie forma diagonal canonică a lui A:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

4.6. Calculul factorilor invarianți

Fie K un corp comutativ şi V un spațiu vectorial peste K de dimensiune n. Fie $B = \{e_1, e_2, \dots, e_n\}$ o bază a lui V şi fie $u: V\to V$ o transformare liniară. Notăm cu $M_B(u) = (a_{ij})_{1\le i,j\le n}$ matricea lui u în baza B. Deci pentru orice $i \in \{1,2, \dots, n\}$

$$u(e_i) = \sum_{i=1}^{n} a_{ij}e_j .$$

Vom arăta că pentru calculul factorilor invarianți ai transformării liniare u, adică al factorilor invarianți ai K[X]-modulului V asociat lui u, se poate folosi matricea $M_B(u)$. Reamintim că V este K[X]-modul înzestrat cu adunarea vectorilor (din V) şi operație algebrică externă:

$$K[X] \times V \to V,\ (P, x) \to P\cdot x$$

$$P\cdot x = \alpha_0 x + \alpha_1 u(x) + \dots + \alpha_s u^s(x),$$

pentru $P = \alpha_0 + \alpha_1 X + \dots + \alpha_s X^s \in K[X]$.

Fie F un K[X]-modul liber de rang n, şi fie $\{\omega_1, \omega_2, \dots, \omega_n\}$ o bază a sa. Din teorema 4.2.17 rezultă că există un morfism de K[X]-module

$\varphi : F \to V$ astfel încât $\varphi(\omega_i) = e_i$ pentru orice $1 \le i \le n$.

Considerăm K[X] -modulul $L = \mathrm{Ker}\ \varphi$ şi notăm

$$y_i = X\omega_i - \sum_{j=1}^{n} a_{ij}\omega_j \text{ pentru orice } 1 \le i \le n.$$

Cu aceste notații putem scrie :

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = (XI_n - M_B(u)) \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

Demonstrăm că $\{y_1, y_2, \ldots, y_n\}$ este o bază a K[X] - modulului L. Arătăm că mai întâi că $y_i \in L$ (adică $\varphi(y_i) = 0$) pentru orice $1 \le i \le n$:

$$\varphi(y_i) = \varphi(X\omega_i - \sum_{j=1}^{n} a_{ij}\omega_j) = X\cdot\varphi(\omega_i) - \sum_{j=1}^{n} a_{ij}\varphi(\omega_j)$$

$$= X\cdot e_i - \sum_{j=1}^{n} a_{ij}e_j = u(e_i) - u(e_i) = 0.$$

Fie $y \in F$. Deoarece $\{\omega_1, \omega_2, \ldots, \omega_n\}$ este o bază a lui F, rezultă că există $P_1, P_2, \ldots, P_n \in K[X]$ astfel încât

$$y = P_1\cdot\omega_1 + P_2\cdot\omega_2 + \ldots + P_n\cdot\omega_n .$$

Din $y_i = X\omega_i - \sum_{j=1}^{n} a_{ij}\omega_j$, rezultă că $X\omega_i = y_i - \sum_{j=1}^{n} a_{ij}\omega_j$ pentru orice $1 \le i \le n$.

Prin aplicarea repetată a acestor relații, rezultă că există polinoamele $Q_1, Q_2, \ldots, Q_n \in K[X]$ şi scalarii $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ astfel încât:

$$y = \sum_{i=1}^{n} Q_i y_i + \sum_{i=1}^{n} \alpha_i\omega_i .$$

Deoarece $\varphi(y) = 0$ ($y \in L$), avem

$$0 = \varphi(\sum_{i=1}^{n} Q_i y_i + \sum_{i=1}^{n} \alpha_i\omega_i) = \sum_{i=1}^{n} Q_i \cdot \varphi(y_i) + \sum_{i=1}^{n} \alpha_i\varphi(\omega_i)$$

$$= \sum_{i=1}^{n} \alpha_i\varphi(\omega_i) = \sum_{i=1}^{n} \alpha_i e_i$$

Cum $\{e_1, e_2, \ldots, e_n\}$ este liniar independentă (fiind bază a spațiului vectorial V peste K), obținem $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. În consecință,

$$y = \sum_{i=1}^{n} Q_i y_i ,$$

şi deci $\{y_1, y_2,\ldots, y_n\}$ este sistem de generatori pentru K[X] - modulul L.

Rămâne să arătăm că $\{y_1, y_2,\ldots, y_n\}$ este liniar independentă. Fie polinoamele $P_1, P_2, \ldots, P_n \in K[X]$ astfel încât:

$$P_1 \cdot y_1 + P_2 \cdot y_2 + \ldots + P_n \cdot y_n = 0.$$

Presupunem prin absurd că nu toate polinoamele $P_1, P_2, \ldots, P_n$ sunt nule. Fie P_s unul dintre polinoamele de grad maxim dintre $P_1, P_2, \ldots, P_n$. Avem

$$P_s y_s = -\sum_{\substack{i=1\\ i\neq s}}^{n} P_i y_i \iff$$

$$P_s(X\omega_s - \sum_{j=1}^{n} a_{sj}\omega_j) = -\sum_{\substack{i=1\\ i\neq s}}^{n} P_i\left(X\omega_i - \sum_{j=1}^{n} a_{ij}\omega_j\right) \iff$$

$$(XP_s)\omega_s - \sum_{j=1}^{n} a_{sj}P_s\omega_j = -\sum_{\substack{i=1\\ i\neq s}}^{n} (XP_i)\omega_i + \sum_{\substack{i=1\\ i\neq s}}^{n}\sum_{j=1}^{n} a_{ij}P_i\omega_j \iff$$

$$(XP_s - a_{ss}P_s)\omega_s - \sum_{\substack{j=1\\ j\neq s}}^{n} a_{sj}P_s\omega_j = -\sum_{\substack{i=1\\ i\neq s}}^{n} (XP_i)\omega_i + \sum_{\substack{i=1\\ i\neq s}}^{n}\sum_{\substack{j=1\\ j\neq s}}^{n} a_{ij}P_i\omega_j + \sum_{\substack{i=1\\ i\neq s}}^{n} a_{is}P_i\omega_s \iff$$

$$(XP_s - a_{ss}P_s - \sum_{\substack{i=1\\ i\neq s}}^{n} a_{is}P_i)\omega_s = \sum_{\substack{i=1\\ i\neq s}}^{n} (XP_i)\omega_i + \sum_{\substack{i=1\\ i\neq s}}^{n}\sum_{\substack{j=1\\ j\neq s}}^{n} a_{ij}P_i\omega_j + \sum_{\substack{j=1\\ j\neq s}}^{n} a_{sj}P_s\omega_j \iff$$

Deoarece $\{\omega_1, \omega_2,\ldots, \omega_n\}$ este liniar independentă (fiind bază a K[X]-modulului F), coeficientul lui ω_s dintr-o combinaţie liniară nulă este nul:

$$XP_s - a_{ss}P_s - \sum_{\substack{i=1\\ i\neq s}}^{n} a_{is}P_i = 0 \iff XP_s = a_{ss}P_s + \sum_{\substack{i=1\\ i\neq s}}^{n} a_{is}P_i \iff XP_s = \sum_{i=1}^{n} a_{is}P_i$$

De aici, obţinem că

$$\mathrm{grad}(XP_s) \leq \max\{\mathrm{grad}(P_i),\ 1 \leq i \leq n\},$$

ceea ce reprezintă a contradicţie cu alegerea polinomului P_s. În consecinţă, $\{y_1, y_2,\ldots, y_n\}$ este liniar independentă.

Teorema 4.6.1. *Fie K un corp comutativ şi V un spaţiu vectorial peste K de dimensiune n. Fie u: V→ V o transformare liniară. Atunci factorii invarianţi ai transformării liniare u coincid cu polinoamele de grad mai mare ca zero din matricea diagonal canonică aritmetic echivalentă cu matricea*

$$XI_n - A \in M_{n,n}(K[X]),$$

unde $A= (a_{ij})_{1\le i,j\le n}$ *este matricea lui u în bază oarecare B a lui V.*

Demonstraţie. Folosim notaţiile de la începutul acestei secţiuni. Deoarece L este un K[X]-submodul liber al lui F, conform teoremei 4.2.18, există o bază $\{z_1, z_2, \ldots, z_n\}$ a lui L şi o bază $\{w_1, w_2, \ldots, w_n\}$ a lui F astfel încât

$$z_i = d_i w_i, \text{ pentru orice } 1 \le i \le n$$

unde $d_i \in K[X]$, $d_i \neq 0$ pentru orice $1 \le i \le n$ şi $d_1 \mid d_2 \mid\ldots \mid d_n$. Factorii invarianţi ai K[X]-modulului V = φ(F) (deci factorii invarianţi ai transformării liniare u) coincid cu polinoamele d_i neinversabile în K[X], deci cu polinoamele d_i de grad mai mare decât zero (vezi demonstraţiile 2.4/pg. 206 şi 2.7/p. 209 [4]). Să arătăm acum că matricea sub formă diagonal canonică

$$D = \begin{pmatrix} d_1 & & 0 \\ & d_2 & \\ & & \ddots & \\ 0 & & & d_n \end{pmatrix}$$

este aritmetice echivalentă cu matricea

$$XI_n - A = \begin{pmatrix} X - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & X-a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & X - a_{nn} \end{pmatrix} \in M_{n,n}(K[X])$$

Deoarece $z_i = d_i w_i$, pentru orice $1 \le i \le n$, putem scrie

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = D \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

Pe de altă parte, deoarece $\{z_1, z_2, \dots, z_n\}$ şi $\{y_1, y_2, \dots, y_n\}$ sunt baze ale lui L, rezultă că există o matrice inversabilă $U_0 \in M_{n,n}(K[X])$ astfel încât

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = U_0 \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

(putem folosi un raționament asemănător celui utilizat în secțiunea 1. 4. pentru stabilirea matricei de trecere de la o bază la alta a unui spațiu vectorial). Analog, $\{w_1, w_2, \dots, w_n\}$ şi $\{\omega_1, \omega_2, \dots, \omega_n\}$ fiind baze ale lui F, rezultă că există o matrice inversabilă $V_0 \in M_{n,n}(K[X])$ astfel încât

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = V_0 \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

Deci

$$U_0 \underbrace{(XI_n-A) \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}}_{= (y_1, y_2, \dots, y_n)^t} = DV_0 \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

Cum $\{\omega_1, \omega_2, \dots, \omega_n\}$ este liniar independentă, obținem

$$U_0\,(XI_n\text{-}A) = DV_0,$$

sau echivalent $U_0\,(XI_n\text{-}A)\,V_0^{-1} = D$, ceea ce înseamnă că XI_n -A şi D sunt aritmetic echivalente.

Teorema 4.6.2. *Fie K un corp comutativ şi A, B $\in M_{n,n}(K)$. Următoarele afirmații sunt echivalente:*

1. *A şi B sunt matrice asemenea (adică, există o matrice inversabilă T$\in M_{n,n}(K)$ astfel încât $TAT^{-1} = B$).*
2. *XI_n - A şi XI_n -B sunt matrice aritmetic echivalente (adică, există două matrice inversabile U_0, $V_0 \in M_{n,n}(K)$ astfel încât $U_0AV_0 = B$).*

Demonstrație. 1 => 2. Dacă A şi B sunt matrice asemenea, atunci există o matrice inversabilă T$\in M_{n,n}(K)$ astfel încât $TAT^{-1} = B$. Cum T, $T^{-1} \in GL_n(K)$, T, $T^{-1} \in GL_n(K[X])$. Din faptul că,

$$T(XI_n - A)T^{-1} = XI_n - B,$$

rezultă că XI_n - A şi XI_n -B sunt matrice aritmetic echivalente.

2 => 1. Fie V un spațiu vectorial de dimensiune n peste K, B o bază a lui V, şi u,v: V$\rightarrow$ V două transformări liniare astfel încât A $=M_B(u)$ (matricea lui u în baza B) şi $B=M_B(v)$ (matricea lui u în baza B). Deoarece XI_n - A şi XI_n -B sunt matrice aritmetic echivalente, rezultă că u şi v au aceeaşi factori invarianți, şi deci aceeaşi divizori elementari. Ca urmare, $J_u = J_v$ (matricele canonice Jordan ale transformării liniare u şi v coincid). Există bazele B' şi B" astfel încât $M_{B'}(u) = J_u$ şi $M_{B''}(v) = J_v$. Cum A şi J_u reprezintă matricele asociate aceleiaşi transformări liniare u în baze diferite, rezultă că A şi J_u sunt matrice asemenea. La fel, B $=M_B(v)$ şi $M_{B''}(v) =J_v$ sunt asemenea. Obținem că A şi B sunt asemenea (deoarece sunt asemenea cu $J_u = J_v$).

Definiția 4.6.3. ***Fie K un corp comutativ şi A∈$M_{n,n}$(K). Matricea***

$$XI_n - A \in M_{n,n}(K[X])$$

se numeşte matricea caracteristică a lui A.

Fie D ∈ $M_{n,n}$(K[X]) o matrice sub formă diagonal canonică astfel încât D şi A să fie aritmetic echivalente. Cum A poate fi privită ca matricea asociată unei transformări liniare u: V → V (V spațiu vectorial n-dimensional peste corpul K), din demonstrația teorema 4.6.1, deducem că

$$D = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & O \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & d_1 & & & \\ & & & & & d_2 & & \\ & & & & & & \ddots & \\ & O & & & & & & d_m \end{pmatrix}$$

unde d_i, $1 \le i \le m$, sunt polinoame unitare de grad mai mare decât zero cu proprietatea că $d_1 \mid d_2 \mid \ldots \mid d_m$. Polinoamele $d_1, d_2, \ldots, d_m$ se numesc *factorii invarianți* ai matricei A, iar polinoamele π_i^k, $1 \le i \le p$, rezultate din descompunerea polinoamelor $d_1, d_2, \ldots, d_m$ în factori ireductibili neasociați în divizibilitate se numesc *divizori elementari* ai matricei A. Factorii invarianți şi divizorii elementari ai lui A sunt unic determinați dacă cerem să fie polinoame unitare.

Corolarul 4.6.4. *Fie K un corp comutativ şi A, B∈$M_{n,n}$(K). Matricele A şi B au aceiaşi factori invarianți dacă şi numai dacă sunt asemenea.*

Demonstrație. Se aplică teorema 4.6.2.

Corolarul 4.6.5. *Fie K un corp comutativ şi Pentru orice matrice $A \in M_{n,n}(K)$ există o matrice canonică Jordan J_A astfel încât A şi J_A să fie asemenea.*

Demonstrație. Fie V un spațiu vectorial de dimensiune n peste K, B o bază a lui V, şi u: V→ V o transformare liniară astfel încât $A = M_B(u)$ (matricea lui u în baza B). Există o baza B' astfel încât $M_{B'}(u) = J_u$. Cum A şi J_u reprezintă matricele asociate aceleiaşi transformări liniare u în baze diferite, rezultă că A şi J_u sunt matrice asemenea. Luăm $J_A = J_u$.

Definiție 4.6.6. *Fie K un corp comutativ. Se numeşte formă canonică Jordan (peste K) a matricei $A \in M_{n,n}(K)$ o matrice canonică Jordam $J_A \in \in M_{n,n}(K)$ care este asemenea cu A.*

Forma canonică Jordan J_A a matricei A este unică, mai puțin ordinea celulelor pe diagonală.

Algoritm pentru calculul formei canonice Jordan a unei matrice $A \in M_{n,n}(K)$, K corp comutativ

Pas 1. Se aduce matricea caracteristică XI_n - A la forma diagonal canonică

$$D = \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & O & \\ & & & 1 & & & \\ & & & & d_1 & & \\ & & & & & d_2 & \\ & & & & & & \ddots \\ & & O & & & & & d_m \end{pmatrix}$$

Pas 2. Factorii invarianți ai matricei A sunt polinoamele unde d_i, $1 \le i \le m$, (de grad mai mare decât zero)

Pas 3. Se determină divizorii elementari $\pi_i^{k_i}$, $1 \leq i \leq p$, prin descompunerea polinoamelor $d_1, d_2, \ldots, d_m$ în factori ireductibili neasociați în divizibilitate.

Pas 4. Scrierea formei canonice Jordan: pentru fiecare divizor elementar $\pi_i^{k_i}$ se ataşează companionul C_{π_i}, şi cu acest companion se construieşte celula Jordan $J_{\pi_i^{k_i}}$ corespunzătoare lui $\pi_i^{k_i}$. Matricea canonică Jordan se obține aşezând celulele Jordan pe diagonală

$$\begin{pmatrix} J_{\pi_1^{k_1}} & & & \\ & J_{\pi_2^{k_2}} & & 0 \\ & & \ddots & \\ 0 & & & J_{\pi_p^{k_p}} \end{pmatrix}$$

Exemplul 4.6.7. *Să se aducă la forma canonică Jordan (peste **R**) matricea A din $M_{3,3}$(**R**):*

$$A = \begin{pmatrix} 4 & -5 & 2 \\ 5 & -7 & 3 \\ 6 & -9 & 4 \end{pmatrix}$$

Aducem matricea caracteristică XI_3 - A la forma diagonal canonică (utilizând transformări elementare):

$$XI_3 - A = \begin{pmatrix} X-4 & 5 & -2 \\ -5 & X+7 & -3 \\ -6 & 9 & X-4 \end{pmatrix} \underset{C_2 \leftarrow C_2+2C_3}{\sim} \begin{pmatrix} X-4 & 1 & -2 \\ -5 & X+1 & -3 \\ -6 & 2X+1 & X-4 \end{pmatrix}$$

$$\underset{C_1 \leftrightarrow C_2}{\sim} \begin{pmatrix} 1 & X-4 & -2 \\ X+1 & -5 & -3 \\ 2X+1 & -6 & X-4 \end{pmatrix}$$

$$\underset{C_2 \leftarrow C_2 - (X-4)C_1,\ C_3 \leftarrow C_3 + 2C_1}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ X+1 & -X^2+3X-1 & 2X-1 \\ 2X+1 & -2X^2+7X-2 & 5X-2 \end{pmatrix}$$

$$\underset{L_2 \leftarrow L_2 - (X+1)L_1,\ L_3 \leftarrow L_3 + (2X+1)L_1}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2+3X-1 & 2X-1 \\ 0 & -2X^2+7X-2 & 5X-2 \end{pmatrix}$$

$$\underset{L_3 \leftarrow L_3 - 2L_2}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2+3X-1 & 2X-1 \\ 0 & X & X \end{pmatrix}$$

$$\underset{L_2 \leftarrow L_2 - 2L_3}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2+X-1 & -1 \\ 0 & X & X \end{pmatrix}$$

$$\underset{C_2 \leftrightarrow C_3}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -X^2+X-1 \\ 0 & X & X \end{pmatrix}$$

$$\underset{C_3 \leftarrow C_3 + (-X^2+X-1)C_2}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & X & -X^3+X^2 \end{pmatrix}$$

$$\underset{L_3 \leftarrow L_3 + XL_1}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -X^3+X^2 \end{pmatrix}$$

Factorii invarianți pentru A : $X^3 - X^2 = X^2(X-1)$

Divizorii elementari: $X^2,\ X-1$:

Celulele Jordan : $J_{X^2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\qquad J_{X-1} = (\,1\,)$

Deci forma canonică Jordan a matricei A este:

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

Putem aduce matricea caracteristică XI_3 - A la forma diagonal canonică şi folosind minorii. Notăm cu Δ_i cel mai mare divizor comun al minorilor de ordin i ai matricei XI_3 - A ($1 \le i \le 3$).

$$XI_3 - A = \begin{pmatrix} X-4 & 5 & -2 \\ -5 & X+7 & -3 \\ -6 & 9 & X-4 \end{pmatrix}$$

Evident $\Delta_1 = 1$. Cum

$$\begin{vmatrix} X-4 & -2 \\ -5 & -3 \end{vmatrix} = -3X-2 \qquad \begin{vmatrix} 5 & -2 \\ X+7 & -3 \end{vmatrix} = 2X-1$$

sunt minori de ordinul 2 ai matricei XI_3 - A şi sunt primi între ei, rezultă că $\Delta_2 = 1$.

$$\Delta_3 = \begin{vmatrix} X-4 & 5 & -2 \\ -5 & X+7 & -3 \\ -6 & 9 & X-4 \end{vmatrix} = X^3 - X^2$$

Deci $d_1 \sim \Delta_1 = 1$, $d_2 \sim \Delta_2/\Delta_1 = 1$, $d_3 \sim \Delta_3/\Delta_2 = X^3 - X^2$, şi în consecinţă forma diagonal canonică a matricei XI_3 - A este:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3 - X^2 \end{pmatrix}$$

4.7. Valori şi vectori proprii

Fie V un spaţiu vectorial peste un corp comutativ K, şi fie u : V → V o transformare liniară.

Definiţia 4.7.1. *Un scalar $\lambda \in K$ se numeşte valoare proprie (sau caracteristică) a lui u dacă există un vector nenul $x \in V$ astfel încât $u(x) = \lambda x$. Orice vector nenul $x \in V$ astfel cu proprietatea că $u(x) = \lambda x$. se numeşte vector propriu (sau caracteristic) al lui u corespunzător valorii proprii λ.*

Considerăm pe V structura de K[X] - modul definită de adunarea vectorilor din V şi de operaţia algebrică externă:

$$K[X] \times V \to V,\ (P, x) \to P\cdot x$$

$$P\cdot x = \alpha_0 x + \alpha_1 u(x) + \ldots + \alpha_s u^s(x),$$

pentru $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_s X^s$.

Propoziţia 4.7.2. *Fie x un vector din spaţiu vectorial finit dimensional V. Următoarele afirmaţii sunt echivalente:*

1. *Dimensiunea lui $K[X]\cdot x$ privit ca un subspaţiu vectorial al lui V peste K este egală 1.*
2. *$x \neq 0$ şi există un scalar $\lambda \in K$ astfel încât $u(x) = \lambda x$*

Demonstraţie. 1 => 2. Dacă dimensiunea lui $K[X]\cdot x$ privit ca un subspaţiu vectorial al lui V peste K este egală 1, atunci $x \neq 0$ (altfel $K[X]\cdot x = \{0\}$). Pe de altă parte din lema 4.3.4, rezultă că dimensiunea lui $K[X]\cdot x$ privit ca un subspaţiu vectorial al lui V peste K este egală cu gradul polinomului μ_x. Deci μ_x este polinom unitar de grad 1, şi ca urmare există $\lambda \in K$ astfel încât $\mu_x = X - \lambda$. Cum

$0 = \mu_x \cdot x = u(x) - \lambda x$,

obținem că $u(x) = \lambda x$.

2 = > 1. Dacă există un scalar $\lambda \in K$ astfel încât $u(x) = \lambda x$, atunci $u(x) - \lambda x = 0$, şi deci $(X - \lambda)\cdot x = 0$. De aici rezultă că $\mu_x \mid (X-\lambda)$, de unde deducem că $\mathrm{grad}(\mu_x) \leq 1$. Cum V este K[X] modul de torsiune (conform lemei 4.3.2), $\mathrm{Ann}_{K[X]}\{x\} \neq 0$, ceea ce implică $\mathrm{grad}(\mu_x) \geq 1$. În consecință, $\mathrm{grad}(\mu_x) = 1$, şi deci dimensiunea lui $K[X]\cdot x$ privit ca un subspațiu vectorial al lui V peste K este egală 1 (conform lemei 4.3.4).

Definiția 4.7.3. *Un scalar $\lambda \in K$ se numeşte valoare proprie (sau caracteristică) a unei matrice $A \in M_{n,n}(K)$ dacă există un vector nenul $x = (x_1, x_2,\ldots, x_n) \in K^n$ astfel încât $Ax^t = \lambda x^t$. Orice vector nenul $x = (x_1, x_2,\ldots, x_n) \in K^n$ cu proprietatea că $Ax^t = \lambda x^t$ se numeşte vector propriu (sau caracteristic) al lui A corespunzător valorii proprii λ.*

Datorită corespondenței biunivoce dintre endomorfismele unui spațiu vectorial V n-dimensional peste corpul comutativ K, $u : V \to V$, şi matricele $A \in M_{n,n}(K)$, rezultă că un scalar $\lambda \in K$ este valoare proprie pentru $u: V \to V$ dacă şi numai dacă este valoare proprie pentru $M_B(u)^t$, unde $M_B(u)$ este matricea lui u într-o bază oarecare B.

Definiția 4.7.4. *Fie $A \in M_{n,n}(K)$. Polinomul $P_A \in K[X]$:*

$$P_A = \det(XI_n - A) = \begin{vmatrix} X-a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & X - a_{22} & \ldots & -a_{2n} \\ & & & \\ -a_{n1} & -a_{n2} & \ldots & X-a_{nn} \end{vmatrix}$$

$$= X^n - (a_{11} + a_{22} + \ldots + a_{nn})X^{n-1} + \ldots + (-1)^n \det(A)$$

se numeşte polinomul caracteristic al matricei A.

În unele lucrări polinomul caracteristic al matricei A este definit ca

$$det\,(A - XI_n\,) = \begin{vmatrix} a_{11} - X & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - X & \dots & a_{2n} \\ & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} - X \end{vmatrix}$$

$$=(-1)^n\,det\,(XI_n - A)$$

Vom opta pentru prima variantă. Se observă că polinomul caracteristic al matricei A şi cel al matricei A^t coincid.

Propoziția 4.7.5. *Orice două matrice asemenea A, B $\in M_{n,n}(K)$ au polinoame caracteristice egale.*

Demonstrație. Dacă A, B $\in M_{n,n}(K)$ sunt asemenea, atunci există $T \in GL_n(K)$ astfel încât $TAT^{-1} = B$. Avem

$$P_A = det(XI_n - A) = det(T(XI_n - A)T^{-1})$$
$$= det(XI_n - TAT^{-1}) = det(XI_n - B) = P_B.$$

Definiția 4.7.6. *Fie V un spațiu vectorial finit dimensional peste un corp comutativ K şi fie B o bază a lui V. Fie u: V→V o transformare liniară. Se numeşte polinom caracteristic al transformării liniare u polinomul caracteristic al matricei $M_B(u)$ (unde $M_B(u)$ este matricea lui u în baza B). Din propoziția 4.8.5 rezultă că polinomul caracteristic al lui u nu depinde de baza B.*

Propoziția 4.7.7. *Fie V un spațiu vectorial n-dimensional peste corpul comutativ K. Fie d_1, d_2, …, d_m factorii invarianți ai transformării liniare u : V → V (respectiv ai matricei*

$A \in M_{n,n}(K)$). Fie P_u (respectiv, P_A) polinomul caracteristic al transformării liniare u (respectiv, polinomul caracteristic al matricei A) Atunci:

1. *$P_u = d_1 d_2 \ldots d_m$ (respectiv, $P_A = d_1 d_2 \ldots d_m$)*
2. *Dacă μ_u (respectiv, μ_A) este polinomul minimal al lui u (respectiv polinomul minimal al lui A), atunci $\mu_u = d_m$ (respectiv, $\mu_A = d_m$). În consecință, polinoamele minimale divid polinoamele caracteristice.*

Demonstrație. 1. Fie B o bază în V şi fie $M_B(u)$ matricea lui u în baza B. Fie D matricea sub formă diagonal canonică aritmetic echivalentă cu $XI_n - M_B(u)$ (respectiv, cu $XI_n - A$) :

$$D = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & O & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & d_1 & & & \\ & & & & & d_2 & & \\ & & & & & & \ddots & \\ & O & & & & & & d_m \end{pmatrix}$$

Polinoamele unitare d_i, $1 \le i \le m$, de grad mai mare decât zero cu proprietatea că $d_1 \mid d_2 \mid \ldots \mid d_m$, sunt factorii invarianți. Cum $XI_n - M_B(u)$ (respectiv cu $XI_n - A$) şi D sunt aritmetic echivalente, $\det(XI_n - M_B(u))$ (respectiv cu $\det(XI_n - A)$) şi det(D) sunt polinoame asociate în divizibilitate. Fiindcă sunt polinoame unitare, rezultă de fapt că

$$\det(XI_n - M_B(u)) = \det(D) \text{ (respectiv, } \det(XI_n - A) = \det(D)).$$

În consecință, $P_u = d_1 d_2 \ldots d_m$ (respectiv, $P_A = d_1 d_2 \ldots d_m$).

2. Rezultatul se obține din lema 4.3.3.

Teorema 4.7.8. ***(Teorema Hamilton-Cayley)*** *Fie V un spaţiu vectorial finit dimensional peste corpul comutativ K. Orice transformare liniară u : $V \to V$ (respectiv matrice $A \in M_{n,n}(K)$) este rădăcina a polinomului său caracteristic.*

Demonstraţie. Transformarea liniară u (respectiv matricea A) este rădăcină a polinomului ei minimal (din definiţia polinomului minimal). Din propoziţia precedentă rezultă că polinomul minimal divide polinomul caracteristic. Deci, u (respectiv A) este şi rădăcină a polinomului caracteristic.

Alternativ, putem demonstra această teoremă, utilizând doar definiţia polinomului caracteristic. Pentru orice matrice C, notăm cu C^+ matricea formată prin transpunerea lui C şi înlocuirea fiecărui element cu complementul său algebric. Matricea C^+ are proprietatea că $CC^+ = C^+C = \det(C)I_n$. Avem

$$(XI_n - A)^+ = B_{n-1}X^{n-1} + B_{n-2}X^{n-2} + \dots + B_1X + B_0,$$

unde $B_k \in M_{n,n}(K)$ pentru orice $0 \le k \le n$. Pe de altă parte,

$$(XI_n - A)(XI_n - A)^+ = \det(XI_n - A)I_n = P_A(X)I_n =$$
$$= (X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0)I_n.$$

Înlocuind $(XI_n - A)^+$ obţinem,

$$B_{n-1}X^n + (B_{n-2} - AB_{n-1})X^{n-1} + \dots + (B_0 - AB_1)X - AB_0 =$$
$$= (X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0)\, I_n.$$

Identificând coeficienţii, avem

$$\begin{cases} B_{n-1} = I_n \\ B_{n-2} - AB_{n-1} = a_{n-1}I_n \\ B_0 - AB_1 = a_1I_n \\ \dots\dots\dots\dots \\ -AB_0 = a_0I_n \end{cases}$$

Înmulțind la stânga prima egalitate cu A^n, a doua cu A^{n-1}, ş.a.m.d. şi adunându-le obținem:

$$O = A^n + a_{n-1}A^{n-1} + \ldots + a_1A + a_0 I_n.$$

Teorema 4.7.9. ***(Teorema lui Frobenius)*** *Fie V un spațiu vectorial finit dimensional peste corpul comutativ K. Polinomul minimal şi polinomul caracteristic ale unei transformări liniare $u:V\to V$ (respectiv ale unei matrice $A\in M_{n,n}(K)$) au aceiaşi factori ireductibili (peste K).*

Demonstrație. Fie P_u (respectiv μ_u) polinomul caracteristic (respectiv, polinomul minimal) al transformării liniare u. Fie d_1, d_2, …, d_m (polinoame unitare cu proprietatea că $d_1 \mid d_2 \mid \ldots \mid d_m$) factorii invarianți ai transformării liniare u. Atunci din propoziția 4.8.7 rezultă că $P_u = d_1d_2, \ldots d_m$ şi $\mu_u = d_m$. Cum $d_i \mid d_m$ pentru orice $1 \le i \le m$, rezultă că P_u şi μ_u au aceiaşi factori ireductibili. Analog, pentru polinomul caracteristic şi polinomul minimal asociate unei matrice.

Teorema 4.7.10. *Fie V un spațiu vectorial n-dimensional peste corpul comutativ K. Fie P_u polinomul caracteristic al transformării liniare $u:V\to V$ (respectiv, P_A polinomul caracteristic al matricei $A\in M_{n,n}(K)$. Atunci $\lambda\in K$ este o valoare proprie a lui u (respectiv, a lui A) dacă şi numai dacă $P_u(\lambda) = 0$ (respectiv, $P_A(\lambda) = 0$).*

Demonstrație. => Fie μ_u polinomul minimal al lui u. Presupunem că $\lambda\in K$ este o valoare proprie a lui u. Atunci există un vector nenul $x\in V$ astfel încât $u(x) = \lambda x$, ceea ce este echivalent cu $(X-\lambda)\cdot x = 0$. Ținând cont şi de faptul că $x\neq 0$ rezultă că $\mu_x = X - \lambda$. Dar $\mu_x \mid \mu_u \mid P_u$, de unde $P_u(\lambda)$.

<= Fie $\lambda \in K$ astfel încât $P_u(\lambda) = 0$. Atunci $(X - \lambda) \mid P_u$ şi în plus, $(X - \lambda)$ este ireductibil. De aici rezultă că $(X - \lambda) \mid \mu_u$ (din teorema lui Frobenius P_u şi μ_u au aceeaşi factori ireductibili). Fie Q astfel încât $\mu_u = (X - \lambda) Q$. Din lema 4.3.3 rezultă că există $y \in V$ astfel încât $\mu_u = \mu_z$. Dacă luăm $x = Q \cdot y$, atunci $\mu_x = X - \lambda$. Deci $u(x) = \lambda x$ şi $x \neq 0$.

Cum orice matrice A poate fi privită ca matricea asociată unei transformări liniare $u: V \to V$, rezultă că rezultatul demonstrat pentru transformări liniare este valabil şi pentru matrice.

Alternativ, prezentăm o demonstrație a acestei teoreme care nu foloseşte noțiunea de polinom minimal şi teorema lui Frobenius. Scalarul $\lambda \in K$ este valoare proprie pentru $A = (a_{ij})_{1 \le i,j \le n}$ dacă şi numai dacă există un vector nenul $x = (x_1, x_2, \ldots, x_n) \in K^n$ astfel încât $Ax^t = \lambda x^t$, sau echivalent dacă şi numai dacă sistemul

$$\begin{cases} (\lambda - a_{11})x_1 - a_{12}x_2 \quad \ldots - a_{1n}x_n = 0 \\ -a_{21}x_1 + (\lambda - a_{22})x_2 \quad \ldots - a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ -a_{n1}x_1 - a_{n2}x_2 \quad \ldots + (\lambda - a_{nn})x_n = 0 \end{cases}$$

admite soluții nebanale. Condiția necesară şi suficientă că sistemul (liniar şi omogen) de mai sus să admită soluții nebanale este

$$\begin{vmatrix} \lambda - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \ldots & -a_{2n} \\ & & & \\ -a_{n1} & -a_{n2} & \ldots & \lambda - a_{nn} \end{vmatrix} = 0,$$

adică $P_A(\lambda) = 0$.

Observația 4.7.11. În cele ce urmează vom formula rezultatele doar pentru transformări liniare $u: v \to V$ (V spațiu vectorial peste un corp comutativ K). Ele pot fi uşor transpuse şi pentru matrice pătrate cu elemente în corpul K, ținând cont că orice matrice poate fi privită ca matricea asociată unei transformări liniare.

Lema 4.7.12. *Fie V un spațiu vectorial peste un corp comutativ K şi u : V → V o transformare liniară. Dacă λ este o valoare proprie a lui u, atunci mulțimea $V_\lambda = \{x \in V : u(x) = \lambda x\}$ este un subspațiu invariant față de u.*

Demonstrație. Fie x, y $\in V_\lambda$ şi fie α, $\beta \in$ K. Atunci

$$u(\alpha x + \beta y) = \alpha u(x) + \beta u(y) = \alpha(\lambda u(x)) + \beta(\lambda u(y))$$
$$= \lambda(\alpha u(x)) + \lambda(\beta u(y)) = \lambda(\alpha u(x) + \beta u(y))$$
$$= \lambda(u(\alpha x + \beta y)\ ,$$

de unde rezultă că $\alpha x + \beta y \in V_\lambda$, şi deci că V_λ este subspațiu vectorial al lui V. Pentru orice x $\in V_\lambda$, avem

$$u(u(x)) = u(\lambda x) = \lambda u(x),$$

ceea ce înseamnă că u(x) $\in V_\lambda$. Deci $u(V_\lambda) \subset V_\lambda$, sau echivalent V_λ este subspațiu invariant față u.

Definiția 4.7.13. *Fie V un spațiu vectorial peste un corp comutativ K, u : V → V o transformare liniară, şi λ o valoare proprie a lui u. Mulțimea $V_\lambda = \{x \in V : u(x) = \lambda x\}$ se numeşte subspațiu propriu ataşat valorii proprii λ. Dimensiunea subspațiului propriu V_λ (ca subspațiu vectorial a lui V peste K) se numeşte multiplicitatea geometrică a valorii proprii λ. Multiplicitate algebrică a valorii proprii λ este multiplicitatea lui λ ca rădăcină a polinomului caracteristic P_u (reamintim că r este multiplicitatea lui λ ca rădăcină a polinomului P_u sau λ este rădăcină* *multiplă de ordin r a lui P_u, dacă $(x - \lambda)^r / P_u$ iar $(X - \lambda)^{r+1}$ nu divide P_u).*

Lema 4.7.14. *Fie V un spaţiu vectorial peste un corp comutativ K. Pentru orice transformare liniară u : V → V, subspaţiile proprii corespunzătoare la valori proprii distincte, sunt disjuncte (adică intersecţia lor este subspaţiul vectorial {0}).*

Demonstraţie. Fie λ_1 şi λ_2 două valori proprii distincte ale lui u. Presupunem prin absurd că există $x \in V_{\lambda_1} \cap V_{\lambda_2}$, $x \neq 0$. Atunci $u(x) = \lambda_1 x$ şi $u(x) = \lambda_2 x$, de unde, obţinem că $0 = \lambda_1 x - \lambda_2 x = (\lambda_1 - \lambda_2)x$, adică $x = 0$, ceea ce este absurd. Deci $V_{\lambda_1} \cap V_{\lambda_2} = \{0\}$.

Lema 4.7.15. *Fie V un spaţiu vectorial peste un corp comutativ K. Pentru orice transformare liniară u : V → V, vectorii proprii corespunzători la valori proprii distincte, sunt liniar independenţi.*

Demonstraţie. Fie $S = \{x_1, x_2, \ldots, x_m\}$ un sistem de vectori poprii corespunzători respectiv valorilor proprii distincte două câte două $\lambda_1, \lambda_2, \ldots, \lambda_m$. Demonstrăm că S este un sistem liniar independent prin inducţie după m. Pentru m = 1 afirmaţia este evidentă deoarece orice vector propriu este nenul. Presupunem afirmaţia adevărată pentru m -1 şi o demonstrăm pentru m. Fie scalarii $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$ astfel încât:

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m = 0. \qquad (1)$$

Aplicând u în relaţia (1) rezultă

$$\alpha_1 \lambda_1 x_1 + \alpha_2 \lambda_2 x_2 + \ldots + \alpha_m \lambda_m x_m = 0. \qquad (2)$$

Înmulţind relaţia (1) cu λ_m şi scăzând-o din (2), obţinem

$$\alpha_1(\lambda_1 - \lambda_m)x_1 + \alpha_2(\lambda_2 - \lambda_m)x_2 + \ldots + \alpha_{m-1}(\lambda_{m-1} - \lambda_m)x_{m-1} = 0.$$

Din ipoteza de inducție rezultă că

$$\alpha_1(\lambda_1 - \lambda_m) = \alpha_2(\lambda_2 - \lambda_m) = \ldots = \alpha_{m-1}(\lambda_{m-1} - \lambda_m) = 0,$$

şi cum λ_m este diferită de λ_i pentru orice $1 \leq i \leq m-1$, obținem

$$\alpha_1 = \alpha_2 = \ldots = \alpha_{m-1} = 0.$$

Ținând cont din nou de relația (1) rezultă că $\alpha_m x_m = 0$, de unde $\alpha_m = 0$. În consecință sistemul $\{x_1, x_2, \ldots, x_m\}$ este liniar independent.

Propoziția 4.7.16. *Fie V un spațiu vectorial finit dimensional peste corpul comutativ K şi u : V → V o transformare liniară. Multiplicitatea geometrică a oricărei valori proprii a lui u este mai mică sau egală cu multiplicitatea ei algebrică.*

Demonstrație. Fie λ o valoare proprie a lui u şi fie V_λ subspațiu propriu corespunzător lui λ. Notăm cu p multiplicitatea geometrică a lui λ (adică dimensiunea subspațiului V_λ) şi cu m multiplicitatea algebrică a lui λ (adică multiplicitatea lui λ ca rădăcină a polinomului caracteristic P_u). Presupunem prin absurd că $p > m$. Considerăm o bază $\{x_1, x_2, \ldots, x_p\}$ a lui V_λ pe care o completăm până la o bază a lui V: $B=\{x_1, x_2, \ldots, x_p\ x_{p+1}, \ldots, x_n\}$ (n fiind dimensiunea spațiului vectorial V). Deoarece $u(x_i) = \lambda x_i$ pentru orice $1 \leq i \leq p$, matricea lui u în baza B este de forma

$$M_B(u) = \begin{pmatrix} \lambda & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \lambda & \ldots & 0 & 0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & \lambda & 0 & \ldots & 0 \\ \alpha_{p+1,1} & \alpha_{p+1,2} & \ldots & \alpha_{p+1,p} & \alpha_{p+1,p+1} & \ldots & \alpha_{p+1,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{np} & \alpha_{n,p+1} & \ldots & \alpha_{nn} \end{pmatrix}$$

unde $\alpha_{ij} \in$ K oricare ar fi $p+1 \le i \le n$ şi $1 \le j \le n$. Deci polinomul caracteristic al lui u este $P_u = \det(XI_n - M_B(u))$, adică

$$P_u = \begin{vmatrix} X-\lambda & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & X-\lambda & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & X-\lambda & 0 & \dots & 0 \\ -\alpha_{p+1,1} & -\alpha_{p+1,2} & \dots & -\alpha_{p+1,p} & X-\alpha_{p+1,p+1} & \dots & -\alpha_{p+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ -\alpha_{n1} & -\alpha_{n2} & \dots & -\alpha_{np} & -\alpha_{n,p+1} & \dots & X-\alpha_{nn} \end{vmatrix}$$

De aici rezultă că există un polinom $P_1 \in$ K[X] astfel încât

$$P_u = (X - \lambda)^p P1,$$

de unde deducem că multiplicitatea m a lui λ ca rădăcină a lui P_u este mai mare sau egală decât p > m ceea ce este o contradicție. În consecință, presupunerea că p > m este falsă.

4.8. Forma diagonală

Definiția 4.8.1. *Fie V un spațiu vectorial finit dimensional peste corpul comutativ K. O transformare liniară u : V → V se numeşte diagonalizabilă dacă există o bază B a lui V astfel încât matricea lui u în această bază să fie diagonală:*

$$M_B(u) = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

O matrice A $\in M_{n,n}(K)$ se numeşte diagonalizabilă dacă este asemenea cu o matrice diagonală.

Observația 4.8.2. Ca şi în secțiunea precedentă, vom formula rezultatele legate de diagonalizare doar pentru transformări liniare u: v $\rightarrow$ V (V spațiu vectorial finit dimensional peste un corp comutativ K). Ele pot fi uşor transpuse şi pentru matrice pătrate cu elemente în corpul K, ținând cont că orice matrice poate fi privită ca matricea asociată unei transformări liniare.

Teorema 4.8.3. *Fie V un spațiu vectorial finit dimensional peste corpul comutativ K şi u : V $\rightarrow$ V o transformare liniară. Următoarele afirmații sunt echivalente:*

1. u diagonalizabil

2. Rădăcinile polinomului caracteristic P_u sunt în K, şi pentru fiecare valoare proprie a lui u multiplicitatea ei algebrică este egală cu multiplicitatea ei geometrică.

Demonstrație. Fie n dimensiunea spațiului vectorial V peste K.

1 => 2. Dacă u este diagonalizabil, atunci există o bază B = {x_1, x_2, …, x_n} astfel încât matricea lui u în bază B să fie diagonală

$$M_B(u) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \lambda_1 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ & & & & & & & & & \\ 0 & 0 & \dots & \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ & & & & & \ddots & & & & \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & \lambda_p & 0 \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \lambda_p \dots & 0 \\ & & & & & & & & & \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & 0 \dots & \lambda_p \end{pmatrix}$$

unde λ_i de pe diagonală se repetă de m_i pentru orice $1 \le i \le p$, şi $\lambda_i \neq \lambda_j$ pentru orice $i \neq j$. Atunci polinomul caracteristic al lui u este

$$P_u = \det(XI_n - M_B(u)) = \prod_{i=1}^{p}(X-\lambda_i)^{m_i}.$$

Cum $M_B(u) \in M_{n,n}(K)$, $m_1 + m_2 + \ldots + m_p = n$, şi ca urmare polinomul P_u are n rădăcini (deci toate) în corpul K. Fie g_i multiplicitatea geometrică a valorii proprii λ_i, adică dimensiunea subspațiului propriu V_{λ_i}. Din faptul că matricea lui u în baza B are forma de mai sus, rezultă că

$$u(x_j) = \lambda_i x_j \text{ pentru orice } \sum_{k=1}^{i-1} m_k + 1 \le j \le \sum_{k=1}^{i} m_k,$$

şi deci $x_j \in V_{\lambda_i}$ pentru orice $\sum_{k=1}^{i-1} m_k + 1 \le j \le \sum_{k=1}^{i} m_k$. De aici rezultă că dimensiunea lui V_{λ_i} (adică g_i) este mai mare decât m_i. Din propoziția 4.8.16 $g_i \le m_i$. Deci $g_i = m_i$ pentru orice $1 \le i \le p$.

2 => 1. Fie p numărul de rădăcini distincte ale polinomului caracteristic P_u şi $\{\lambda_i : 1 \le i \le p\}$ rădăcinile distincte. Fie m_i multiplicitatea rădăcinii λ_i pentru orice $1 \le i \le p$. Fie B_i o bază pentru subspațiu propriu V_{λ_i} pentru orice $1 \le i \le p$. Fie $B = \{x_1, x_2, \ldots, x_n\}$ o mulțime de vectori din V astfel încât primii m_1 să fie vectorii din B_1, următorii m_2 să fie vectorii din B_2, şi aşa mai departe. Demonstrăm că B este o bază a lui V. Deoarece numărul de vectori din B coincide cu dimensiunea lui V este suficient să arătăm că B este liniar independentă. Fie scalarii $\alpha_1, \ldots, \alpha_n \in K$ astfel încât $\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$. Notăm

$$f_i = \sum_{j=n_i}^{n_{i+1}-1} \alpha_j x_j, \text{ unde } n_i = \sum_{k=1}^{i-1} m_k + 1, \text{ pentru orice } 1 \le i \le p.$$

Avem $f_i \in V_{\lambda_i}$ pentru orice $1 \le i \le p$ şi $f_1 + f_2 + \ldots + f_p = 0$. Nu pot exista vectori f_i nenuli, deoarece vectorii proprii corespunzători la valori proprii distincte sunt liniari independenți. Deci $\sum_{j=n_i}^{n_{i+1}-1} \alpha_j x_j = 0$ pentru orice $1 \le i \le p$. Dar $\{x_{n_i}, x_{n_i+1}, \ldots, x_{n_i+m_i-1}\}$ este o bază în V_{λ_i}, ceea ce implică $\alpha_j = 0$ pentru orice $n_i \le j \le n_{i+1} - 1$. Deci B este o mulțime liniar independentă.

Matricea lui u în baza B este diagonală:

$$M_B(u) = \begin{pmatrix} \lambda_1 & 0 \ldots 0 & 0 \ldots 0\,0 & \ldots 0 \\ 0 & \lambda_1 \ldots 0 & 0 \ldots 0\,0 & \ldots 0 \\ & & & \\ 1 & 0 \ldots \lambda_1 & 0 \ldots 0\,0 & \ldots 0 \\ & & \ddots & \\ 0 & 0 \ldots 0 & 0 \ldots 0 & \lambda_p\, 0 \ldots 0 \\ 0 & 0 \ldots 0 & 0 \ldots 0\;0 & \lambda_p \ldots 0 \\ & & & \\ 0 & 0 \ldots 0 & 0 \ldots 0\;0 & 0 \ldots \lambda_p \end{pmatrix}$$

Corolarul 4.8.4. *Fie V un spațiu vectorial n-dimensional peste corpul comutativ K şi u : V → V o transformare liniară. Dacă u este diagonalizabil şi dacă $\lambda_1, \lambda_2, \ldots, \lambda_p$ sunt cele p valori proprii distincte ale lui u, atunci*

$$V = V_{\lambda_i} \oplus V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_p},$$

unde V_{λ_i} este subspațiul propriu corespunzător lui λ_i pentru orice $1 \le i \le p$.

Demonstrație. Fie B_i o bază pentru subspațiu propriu V_{λ_i} pentru orice $1 \le i \le p$. Fie $B = \{x_1, x_2, \ldots, x_n\}$ o mulțime de vectori din V astfel încât primii m_1 să fie vectorii din B_1, următorii m_2 să fie vectorii din B_2, şi aşa mai departe. Utilizând aceleaşi argumente ca în demonstrația de la 2 => 1 din teorema precedentă, rezultă că B este o bază a lui V.

Teorema 4.8.5. *Fie V un spaţiu vectorial n-dimensional peste un corp comutativ K având mai mult de n elemente. Fie $u : V \to V$ o transformare liniară. Următoarele afirmaţii sunt echivalente:*

1. *u este diagonalizabil*
2. *Există o bază a spaţiului vectorial V formată din vectori proprii ai lui u*
3. *Polinomul minimal al u este de forma*

$$(X - \lambda_1)(X - \lambda_2)\dots(X - \lambda_m)$$

cu $\lambda_i \in K$ pentru orice $1 \le i \le m$, şi $\lambda_i \neq \lambda_j$ pentru $i \neq j$ $(m \le n)$.

4. *Există o transformare liniară $v: V \to V$ cu n valori proprii distincte astfel încât $u \circ v = v \circ u$.*

Demonstraţie. 1 =>2. Fie $B=\{x_1, x_2, \dots, x_n\}$ o bază în care matricea lui u are forma :

$$M_B(u) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Atunci $u(x_i) = \lambda_i x_i$ şi $x_i \neq 0$ pentru orice $1 \le i \le n$. Deci baza este formată din vectori proprii ai lui u.

2 => 1. Fie $B=\{x_1, x_2, \dots, x_n\}$ o bază formată din vectori proprii ai lui u. Atunci pentru orice $1 \le i \le n$, există λ_i astfel încât $u(x_i) = \lambda_i x_i$. Cum matricea lui u în această bază este

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

rezultă că u este diagonalizabil.

1 => 4. Fie $B=\{x_1, x_2, \ldots, x_n\}$ o bază în care matricea lui u este *:*

$$M_B(u) = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Fie $\{\beta_1, \beta_2, \ldots, \beta_n\}$ o submulțime a lui K cu proprietatea că $\beta_i \neq \beta_j$ pentru orice $i \neq j$. Definim $v : V \to V$, prin $v(x_i) = \beta_i x_i$ pentru orice $1 \leq i \leq n$. Atunci $\{\beta_1, \beta_2, \ldots, \beta_n\}$ sunt valorile proprii ale lui v şi

$$u \circ v\,(x_i) = u(\beta_i x_i) = \beta_i \lambda_i x_i = \lambda_i \beta_i x_i =$$

$$= \lambda_i v(x_i) = v(\lambda_i x_i) = v(u(x_i)) = v \circ u(x_i)$$

pentru orice $1 \leq i \leq n$.

4 = > 1. Fie $v: V \to V$ o transformare liniară cu n valori proprii distincte astfel încât $u \circ v = v \circ u$. Fie $\{\beta_1, \beta_2, \ldots, \beta_n\}$ valorile proprii (distincte) ale lui v şi fie B baza lui V formată din vectori proprii ai lui v. Atunci

$$M_B(v) = \begin{pmatrix} \beta_1 & 0 & \ldots & 0 \\ 0 & \beta_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \beta_n \end{pmatrix}$$

Deoarece $u \circ v = v \circ u$, avem $M_B(u)\, M_B(v) = M_B(v)\, M_B(u)$. Dacă $M_B(u) =(\alpha_{ij})_{ij}$ atunci din egalitatea precedentă rezultă că $\alpha_{ij}\beta_j = \beta_i\alpha_{ij}$ pentru orice i şi j. Cum $\beta_i \neq \beta_j$ pentru $i \neq j$, $\alpha_{ij} = 0$ dacă $i \neq j$. Deci matricea lui u în baza B este diagonală.

1 =>3. Fie $B = \{x_1, x_2, \ldots, x_n\}$ o bază astfel încât matricea lui u în bază B să fie

$$M_B(u) = \begin{pmatrix} \lambda_1 & 0 \ldots 0 & 0 \ldots 0\,0 & \ldots 0 \\ 0 & \lambda_1 \ldots 0 & 0 \ldots 0\,0 & \ldots 0 \\ \\ 2 & 0 \ldots \lambda_1 & 0 \ldots 0\,0 & \ldots 0 \\ & & \ddots & \\ 0 & 0 \ldots 0 & 0 \ldots 0 & \lambda_p\, 0 \ldots 0 \\ 0 & 0 \ldots 0 & 0 \ldots 0\,0 & \lambda_p \ldots 0 \\ \\ 0 & 0 \ldots 0 & 0 \ldots 0\,0 & 0 \ldots \lambda_p \end{pmatrix}$$

unde λ_i de pe diagonală se repetă de m_i pentru orice $1 \leq i \leq p$, şi $\lambda_i \neq \lambda_j$ pentru orice $i \neq j$. Arătăm că polinomul minimal al lui u este

$$\mu_u = (X - \lambda_1)(X - \lambda_2)\ldots(X - \lambda_m).$$

Pentru a arăta că $\mu_u(u) = 0$ este suficient să arătăm că $x_i \cdot \mu_u = 0$ pentru orice $1 \leq i \leq n$. Avem

$$\begin{aligned} x_i \cdot \mu_u &= (u(x_i) - \lambda_1 x_i)\ldots(u(x_i) - \lambda_i x_i)\ldots(u(x_i) - \lambda_n x_i) \\ &= (u(x_i) - \lambda_1 x_i)\ldots(\lambda_i x_i - \lambda_i x_i)\ldots(u(x_i) - \lambda_n x_i) \\ &= 0. \end{aligned}$$

Fie $P = \alpha_0 + \alpha_1 X + \ldots + \alpha_s X^s \in K[X]$ cu proprietatea că $P \cdot x = 0$ pentru orice $x \in V$. Pentru orice $1 \leq i \leq n$, din

$$\begin{aligned} P \cdot e_i &= \alpha_0 e_i + \alpha_1 u(e_i) + \ldots + \alpha_s u^s(e_i) \\ &= \alpha_0 e_i + \alpha_1 \lambda_i e_i + \ldots + \alpha_s \lambda_i^s e_i \\ &= (\alpha_0 + \alpha_1 \lambda_i + \ldots + \alpha_s \lambda_i^s) e_i \end{aligned}$$

rezultă că $(\alpha_0 + \alpha_1 \lambda_i + \ldots + \alpha_s \lambda_i^s) e_i = 0$, şi ca urmare $(\alpha_0 + \alpha_1 \lambda_i + \ldots + \alpha_s \lambda_i^s) = 0$. Am obținut astfel că λ_i este rădăcina a lui P, ceea ce implică $(X - \lambda_i) \mid P$ pentru orice $1 \leq i \leq n$. Cum $\lambda_i \neq \lambda_j$ pentru orice $i \neq j$, rezultă $(X - \lambda_1)(X - \lambda_2)\ldots(X - \lambda_m) \mid P$, adică $\mu_u \mid P$.

3 =>1. Fie d_1, d_2, …, d_m factorii invarianți ai transformării liniare u:V $\rightarrow$ V. Din propoziția 4.8.7 rezultă că $\mu_u = d_m$ (μ_u fiind polinomul minimal al lui u). Deoarece $d_m =(X - \lambda_1)(X - \lambda_2)\ldots(X - \lambda_m)$ cu $\lambda_i \in K$ pentru orice $1 \leq i \leq m$, $m \leq n$ şi $\lambda_i \neq \lambda_j$ pentru $i \neq j$, rezultă că pentru $k < m$ factorul invariant d_k este fie 1 fie un produs de polinoame de forma λ_{i_j} cu λ_{i_j} distincte. Deci divizorii elementari sunt de forma $X - \lambda_{i_j}$. Matricea canonică Jordan este în acest caz o matrice diagonală:

$$J_u = \begin{pmatrix} \lambda_1 & 0 \ldots 0 & 0 & \ldots 0\ 0 & \ldots 0 \\ 0 & \lambda_1 \ldots 0 & 0 & \ldots 0\ 0 & \ldots 0 \\ \\ 3 & 0\ \ldots \lambda_1 & 0 & \ldots 0\ 0 & \ldots 0 \\ & & \ddots & & \\ 0 & 0 \ldots\ 0 & 0 \ldots 0 & \lambda_m\ 0 \ldots 0 \\ 0 & 0 \ldots\ 0 & 0 \ldots 0 & 0\ \lambda_m \ldots 0 \\ \\ 0 & 0 \ldots\ 0 & 0 \ldots 0 & 0\ 0 \ldots \lambda_m \end{pmatrix}$$

Fiecare valoare proprie λ_i se repetă pe diagonală de un număr de ori egal cu numărul de divizori elementari ai lui u de forma $X - \lambda_i$.

4.9. Endomorfisme peste corpuri algebric închise

Scopul acestui subcapitol este prezentarea unei alte modalități de aducere la forma canonică Jordan a unui endomorfism u : V $\rightarrow$ V, cu V spațiu vectorial peste corpul comutativ algebric închis K.

Teorema 4.9.1. *Fie V un spațiu vectorial n-dimensional peste un corp comutativ K. Fie u : V → V un endomorfism al cărui polinom caracteristic este*

$$P_u(X) = (X-\lambda_1)^{n_1}\ (X-\lambda_2)^{n_2} \ldots\ (X-\lambda_m)^{n_m},$$

unde $\lambda_i \neq \lambda_j$ *pentru orice* $i \neq j$ *şi* $\sum_{i=1}^{m} n_i = n$. *Dacă* $V_i = \mathrm{Ker}(u-\lambda_i I)^{n_i}$ *pentru orice* $1 \leq i \leq m$, *atunci*

1. V_i *este subspațiu invariant la u pentru orice* $1 \leq i \leq m$
2. $V = V_1 \oplus V_2 \oplus \ldots \oplus V_m$

Demonstrație. 1. Fie $x \in V_i$. Atunci $(u-\lambda_i I)^{n_i}(x) = 0$ şi deci

$$(u-\lambda_i I)^{n_i}(u(x)) = u((u-\lambda_i I)^{n_i}(x)) = u(0) = 0,$$

de unde rezultă că $u(x) \in V_i$.

2. Considerăm polinoamele $P_i(X) = P_u(X)/(X-\lambda_i)^{n_i}$, $1 \leq i \leq m$. Cum $\lambda_i \neq \lambda_j$ pentru orice $i \neq j$, polinoamele P_i sunt prime între ele. Prin urmare, există polinoamele $Q_1, .., Q_m$ astfel încât $Q_1P_1 + Q_2P_2 + \ldots + Q_mP_m = 1$. De aici rezultă că $Q_1(u)P_1(u) + Q_2(u)P_2(u) + \ldots + Q_m(u)P_m(u) = I$. Pentru orice $x \in V$, notăm $x_i = (Q_i(u)P_i(u))(x)$, $1 \leq i \leq m$. Avem $x = x_1 + x_2 + \ldots + x_m$. Pe de altă parte $(u-\lambda_i I)^{n_i}(x_i) = Q_i(u)(u-\lambda_i I)^{n_i}\ P_i(u)(x) = Q_i(u)P_u(u)(x) = 0$, deoarece $P_u(u) = 0$ conform teoremei Hamilton-Cayley. Deci $x_i \in V_i$. Am arătat astfel că $V = V_1 + V_2 + \ldots + V_m$ Cum $\lambda_i \neq \lambda_j$ pentru $i \neq j$, avem $V_i \cap \sum_{j\neq i} V_j = \phi$ (demonstrație prin inducției după m) şi deci suma subspațiilor V_i este directă.

Teorema 4.9.2. *Fie V un spațiu vectorial n-dimensional peste un corp comutativ K algebric închis. Fie u : V → V un endomorfism Atunci există o bază B = {e_1, e_2, ..., e_n} a lui V astfel încât matricea asociată lui u în baza B să fie J_u (matricea canonică Jordan asociată lui u).*

Demonstrație. Fie P_u polinomul caracteristic. Deoarece K algebric închis, rezultă că P_u poate fi scris sub forma

$$P_u(X) = (X-\lambda_1)^{n_1}\ (X-\lambda_2)^{n_2} \dots\ (X-\lambda_m)^{n_m},$$

unde $\lambda_i \neq \lambda_j$ pentru orice $i \neq j$ şi $\sum\limits_{i=1}^{m} n_i = n$. Dacă $V_i = \mathrm{Ker}(u-\lambda_i I)^{n_i}$ ($1 \leq i \leq m$), atunci conform teoremei precedente, V_i este invariant la u. Notăm cu u_i endomorfismul indus de u pe V_i. Se observă uşor că $u_i - \lambda_i I$ este un endomorfism nilpotent. Conform teoremei 3.5.18 există o bază B_i a lui V_i astfel încât matricea lui u_i în raport cu baza B_i să aibă forma

$$M_{B_i}(u_i - \lambda_i I) = \begin{pmatrix} 0 & \xi_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \xi_2 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & \xi_{ni-1} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

unde $\xi_i \in \{0, 1\}$ pentru orice $1 \leq i \leq n_i-1$. Prin urmare matricea lui u_i în raport cu baza B_i este

$$M_{B_i}(u_i) = \begin{pmatrix} \lambda_i & \xi_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda_i & \xi_2 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \lambda_i & \xi_{ni-1} \\ 0 & 0 & 0 & 0 & \dots & 0 & \lambda_i \end{pmatrix}$$

unde $\xi_i \in \{0, 1\}$ pentru orice $1 \leq i \leq n_i-1$. Deci matricea lui u în raport cu baza $B = B_1 \cup B_2 \cup \dots \cup B_m$ are forma canonică Jordan.

4. 10. Exerciții

1. Să se scrie forma canonică Jordan peste corpul K (K = **Q**, **R**, **C**) a unei matrice A care are proprietatea că factorii invarianți (ai matricei XI_n - A) sunt

$X^2 + 4$, $(X^2 - 5)(X^2 + 4)^2$

R: Notăm cu DE_K divizorii elementari ai matricei A (peste corpul K):

$DE_{\mathbf{Q}} = \{ X^2 + 4, (X^2 - 5), (X^2 + 4)^2 \}$

$DE_{\mathbf{R}} = \{ X^2 + 4, X - \sqrt{5}, X + \sqrt{5}, (X^2 + 4)^2\}$

$DE_{\mathbf{C}} = \{ X - 2i, X + 2i, X - \sqrt{5}, X + \sqrt{5}, (X - 2i)^2, (X + 2i)^2\}$

Pentru K = **Q**,

$$C_{(x^2+4)} = \begin{pmatrix} 0 & 1 \\ -4 & 0 \end{pmatrix} \qquad C_{(x^2-5)} = \begin{pmatrix} 0 & 1 \\ 5 & 0 \end{pmatrix}$$

$$J_{(x^2+4)^2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4 & 0 \end{pmatrix}$$

Forma canonică Jordan a lui A este

$$J_A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 0 \end{pmatrix}$$

În cazul K = **R** forma canonică Jordan a lui A este

$$
J_A = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \sqrt{5} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -\sqrt{5} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & -4 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & -4 & 0
\end{pmatrix}
$$

În cazul K = **C** forma canonică Jordan a lui A este

$$
J_A = \begin{pmatrix}
2i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -2i & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \sqrt{5} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -\sqrt{5} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2i & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 2i & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -2i & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -2i
\end{pmatrix}
$$

2. Fie V un spațiu vectorial de dimensiune finită peste corpul C şi fie $u:V\to V$ un endomorfism. Să se arate că există două endomorfisme $v,w:V\to V$ astfel încât u = v +w, v diagonalizabil şi w nilpotent.

R: Există o bază B în care matricea asociată lui u are forma canonică Jordan. Deoarece celulele Jordan peste **C** sunt de forma

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

rezultă că

$$
J_u = \begin{pmatrix}
\lambda_1 & \xi_1 & 0 & 0 & \ldots & 0 & 0 \\
0 & \lambda_2 & \xi_2 & 0 & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & \ldots & \lambda_{n-1} & \xi_{n-1} \\
0 & 0 & 0 & 0 & \ldots & 0 & \lambda_n
\end{pmatrix}
$$

unde $\xi_i \in \{0, 1\}$ pentru orice $1 \le i \le n-1$. Luăm v endomorfismul corespunzător matricei

$$
\begin{pmatrix}
\lambda_1 & 0 & 0 & 0 & \ldots & 0 & 0 \\
0 & \lambda_2 & 0 & 0 & \ldots & 0 & 0 \\
 & & & & & & \\
0 & 0 & 0 & 0 & \ldots & \lambda_{n-1} & 0 \\
0 & 0 & 0 & 0 & \ldots & 0 & \lambda_n
\end{pmatrix}
$$

$$\begin{pmatrix} \\ \cdots\cdots\cdots\cdots \\ \\ \end{pmatrix}$$

în baza B. Luăm w endomorfismul corespunzător matricei

$$\begin{pmatrix} 0 & \xi_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \xi_2 & 0 & \ldots & 0 & 0 \\ \cdots & & & & & & \\ 0 & 0 & 0 & 0 & \ldots & 0 & \xi_{n-1} \\ 0 & 0 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}$$

în baza B. Avem u = v + w, v diagonalizabil şi w nilpotent.

3. Să se determine valorile proprii şi subspațiile proprii ale matricei

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

R: Valorile proprii sunt rădăcinile polinomului caracteristic $P_A(X) = \det(XI_3 - A)$. Avem

$$P_A(\lambda) = \begin{vmatrix} \lambda-5 & 2 & 6 \\ 0 & \lambda-1 & 0 \\ -2 & 1 & \lambda+2 \end{vmatrix} = (\lambda-1)\begin{vmatrix} \lambda-5 & 6 \\ -2 & \lambda+2 \end{vmatrix}$$

$$=(\lambda-1)(\lambda^2 -3\lambda -10 +12) = (\lambda-1)(\lambda-1)(\lambda-2)$$

Obținem valorile proprii $\lambda_1 = 1$ (cu multiplicitatea algebrică 2) şi $\lambda_2 = 2$. Pentru o valoare proprie λ, vectorii proprii sunt dați de soluțiile $x = (x_1, x_2, x_3)$ ale sistemului $(\lambda I_3 - A)x^t = 0$. Pentru $\lambda_1 = 1$ obținem

$$\begin{cases} -4x_1 + 2x_2 + 6x_3 = 0 \\ 0x_1 + 0x_2 + 0x_3 = 0 \\ -2x_1 + x_2 + 3x_3 = 0 \end{cases}$$

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

Deci subspațiul propriu asociat lui λ_1 este

$$V_{\lambda_1} = \{(\alpha, 2\alpha\text{-}3\beta, \beta), \alpha, \beta \in \mathbf{R}\}$$

O bază a acestui subspațiu este $B_1 = \{(1, 2, 0), (0, -3, 1)\}$

Similar, pentru $\lambda_2 = 2$ obținem

$$\begin{cases} -3x_1 + 2x_2 + 6x_3 = 0 \\ 0x_1 + x_2 + 0x_3 = 0 \\ -2x_1 + x_2 + 4x_3 = 0 \end{cases}$$

$$\begin{cases} x_1 = 2\alpha \\ x_2 = 0 \\ x_3 = \alpha \end{cases}$$

Deci subspațiul propriu asociat lui λ_2 este

$$V_{\lambda_2} = \{(2\alpha, 0, \alpha), \alpha \in \mathbf{R}\}$$

O bază a acestui subspațiu este $B_2 = \{(2, 0, 1)\}$

4. Să se arate că matricea A este diagonalizabilă şi să se calculeze A^n, $n \in \mathbf{N}$.

$$A = \begin{pmatrix} 15 & -8 & -24 \\ 0 & -1 & 0 \\ 8 & -4 & -13 \end{pmatrix}$$

R: Conform teoremei 4.8.3 pentru a arăta ca A este diagonalizabilă este necesar şi suficient să arătăm că multiplicitatea algebrică a fiecărei valori proprii a lui A este egală cu multiplicitatea geometrică. Valorile proprii sunt rădăcinile polinomului caracteristic $P_A(X) = \det(XI_3 - A)$. Avem

$$P_A(\lambda) = \begin{vmatrix} \lambda-15 & 8 & 24 \\ 0 & \lambda+1 & 0 \\ -8 & 4 & \lambda+13 \end{vmatrix} = (\lambda+1)\begin{vmatrix} \lambda-15 & 24 \\ -8 & \lambda+13 \end{vmatrix}$$

$$=(\lambda+1)(\lambda^2 -2\lambda -195 +192) = (\lambda+1)(\lambda+1)(\lambda-3)$$

Obținem valorile proprii $\lambda_1 = -1$ (cu multiplicitatea algebrică 2) şi $\lambda_2 = 3$. Determinăm vectorii proprii asociați lui $\lambda_1 = -1$ obținem

$$\begin{cases} -16x_1 + 8x_2 + 24x_3 = 0 \\ 0x_1 + 0x_2 + 0x_3 = 0 \\ -8x_1 + 4x_2 + 12x_3 = 0 \end{cases}$$

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

Deci subspațiul propriu asociat lui λ_1 este

$$V_{\lambda_1} = \{(\alpha, 2\alpha-3\beta, \beta), \alpha, \beta\in \mathbf{R}\}$$

O bază a acestui subspațiu este $B_1 =\{(1, 2, 0), (0, -3, 1)\}$, în consecință multiplicitatea geometrică a lui λ_1 este 2. În cazul valorii proprii λ_2 evident multiplicitatea algebrică = multiplicitatea geometrică =1. Deci matricea A este diagonalizabilă şi are forma diagonală,

$$D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Matricea A poate fi privită ca transpusa matricei unui endomorfism cărui într-o bază B (formată din vectori proprii ai lui A) îi corespunde matricea D. Determinăm matricea de trecere de la baza canonică la baza B. Mai este necesar un vector propriu asociat lui $\lambda_2 = 3$:

$$\begin{cases} -12x_1 + 8x_2 + 24x_3 = 0 \\ 0x_1 + 4x_2 + 0x_3 = 0 \\ -8x_1 + 4x_2 + 16x_3 = 0 \end{cases}$$

$$\begin{cases} x_1 = 2\alpha \\ x_2 = 0 \\ x_3 = \alpha \end{cases}$$

Deci subspațiul propriu asociat lui λ_2 este

$$V_{\lambda_2} = \{(2\alpha, 0, \alpha), \alpha\in \mathbf{R}\}$$

O bază a acestui subspațiu este $B_2 =\{(2, 0, 1)\}$. Matricea de trecere de la baza canonică la baza B este

$$C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -3 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

Avem $CA^tC^{-1} = D$, sau echivalent $(C^t)^{-1}AC^t = D$. Ținând cont că $A = C^tD(C^t)^{-1}$, rezultă că $A^n = C^tD^n(C^t)^{-1}$,

$$A^n = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -3 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & (-1)^n & 0 \\ 0 & 0 & (-3)^n \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ 2 & -3 & 0 \\ 0 & 1 & 1 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 0 & 2 \\ 2 & -3 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} (-1)^n & 0 & 0 \\ 0 & (-1)^n & 0 \\ 0 & 0 & (-3)^n \end{pmatrix} \begin{pmatrix} -3 & 2 & 6 \\ -2 & 1 & 4 \\ 2 & -1 & -3 \end{pmatrix}$$

$$= \begin{pmatrix} -3(-1)^n +4(-3)^n & 2(-1)^n - 2(-3)^n & 6(-1)^n -6(-3)^n \\ 0 & (-1)^n & 0 \\ -2(-1)^n+2(-3)^n & (-1)^n-(-3)^n & 4(-1)^n-3(-3)^n \end{pmatrix}$$

5. Să se studieze posibilitatea reducerii la forma canonică a următoarei matrice:

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

R: Conform teoremei 4.8.3 pentru a arăta ca A este diagonalizabilă este necesar şi suficient să arătăm că multiplicitatea algebrică a fiecărei valori proprii a lui A este egală cu multiplicitatea geometrică. Valorile proprii sunt rădăcinile polinomului caracteristic $P_A(X) = \det(XI_3-A)$. Avem

$$P_A(\lambda) = \begin{vmatrix} \lambda-3 & -1 & -2 \\ -4 & \lambda-3 & -4 \\ -4 & -1 & \lambda+2 \end{vmatrix} = \lambda^3-4\lambda^2+5\lambda-2 =(\lambda-1)^2(\lambda-2)$$

Obținem valorile proprii $\lambda_1 = 1$ (cu multiplicitatea algebrică 2) şi $\lambda_2 =3$. Determinăm vectorii proprii asociați lui $\lambda_1 = 1$ obținem

$$\begin{cases} -2x_1 - x_2 - 2x_3 = 0 \\ -4x_1 - 2x_2 - 4x_3 = 0 \\ -4x_1 - x_2 + 3x_3 = 0 \end{cases}$$

$$\begin{cases} x_1 = 5\alpha \\ x_2 = -14\alpha \\ x_3 = 2\alpha \end{cases}$$

Deci subspațiul propriu asociat lui λ_1 este

$$V_{\lambda_1} = \{(5\alpha, -14\alpha, 2\alpha), \alpha\in \mathbf{R}\}$$

O bază a acestui subspațiu este $B_1 =\{(5, -14, 2)\}$, în consecință multiplicitatea geometrică a lui λ_1 este 1 mai mică strict decât multiplicitatea algebrică. În consecință, matricea A nu este diagonalizabilă.

6. Folosind teorema Hamilton-Cayley să se calculeze inversa matricei A în funcție de puterile sale:

$$A= \begin{pmatrix} -1 & 2 & -3 & 4 & \ldots & (-1)^n n \\ 0 & -1 & 2 & -3 & \ldots & (-1)^{n-1}n-1 \\ 0 & 0 & -1 & 2 & \ldots & (-1)^{n-2}n-2 \\ \cdots & & & & & \\ 0 & 0 & 0 & \ldots & & -1 \end{pmatrix}$$

R: Polinomul caracteristic al matricei A este $P(X) = (X+1)^n$. Conform teoremei Hamilton-Cayley, $(A+I_n)^n = O$, sau echivalent

$$A^n + C_n^1 A^{n-1} + C_n^2 A^{n-2} + \ldots + C_n^{n-1} A + I_n = O.$$

Înmulțind această egalitate cu A^{-1}, obținem $A^{-1} = - A^{n-1} - C_n^1 A^{n-2} - C_n^2 A^{n-3}$ $- \ldots - C_n^{n-1} I_n$.

7. Să se calculeze e^A pentru

$$A = \begin{pmatrix} 3 & 4 & 6 \\ 4 & 9 & 12 \\ -4 & -7 & -10 \end{pmatrix}$$

unde $e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k$.

R: Orice polinom de matrice A ($A \in M_{n,n}(K)$) poate fi exprimat printr-un polinom de grad cel mult n-1. Într-adevăr, fie $P_A(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ polinomul caracteristic al matricei A. Conform teoremei Hamilton-Cayley, $P_A(A) = O$, şi deci $A^n = - a_{n-1}A^{n-1} + \ldots + a_1A + a_0I_n$. Puterile A^{n+p} se exprimă recursiv cu ajutorul puterilor A^{n-1}, A^{n-2}, .., A, I_n. De asemenea seriile de matrice se reduc la polinom (de matrice) de grad cel mult n-1 (dacă seria este convergentă, atunci şi coeficienții polinomului sunt serii convergente). Dacă f este o serie de matrice A şi dacă valorile proprii (λ_1, …, λ_2) ale matricei A sunt distincte, atunci polinomul de grad n-1 poate fi scris sub formă Lagrange: f(A) = $\sum_{j=1}^{n} Z_j f(\lambda_j)$, unde $Z_j = \frac{(A - \lambda_1 I_n)\ldots(\lambda_j - \lambda_{j-1} I_n)(\lambda_j - \lambda_{j+1} I_n)\ldots(\lambda_j - \lambda_n I_n)}{(\lambda_j - \lambda_1)\ldots(\lambda_j - \lambda_{j-1})(\lambda_j - \lambda_{j+1})\ldots(\lambda_j - \lambda_n)}$

nu depinde de f, şi deci poate fi aflat prin particularizarea lui f.

Să determinăm valorile proprii ale matricei. Avem

$$P_A(\lambda) = \begin{vmatrix} \lambda-3 & -4 & -6 \\ -4 & \lambda-9 & -12 \\ 4 & 7 & \lambda+10 \end{vmatrix} = \lambda^3-2\lambda^2-\lambda+2 =(\lambda-1)(\lambda+1)(\lambda-2)$$

Obținem valorile proprii $\lambda_1 = 1$, $\lambda_2 =-1$, $\lambda_3 = 2$. Deoarece sunt distincte $f(A) = Z_1f(\lambda_1) + Z_2f(\lambda_2) + Z_3f(\lambda_3)$. Matricele Z_1, Z_2, Z_3 nu depind de f, şi de aceea pentru a le afla particularizăm pe f prin : $f(z) = z-1$, $f(z) = z+1$, $f(z) = z^2$. Obținem

$$-2Z_2 + Z_3 = A-I_3$$

$$2Z_1 + 3Z_3 = A+I_3$$

$$Z_1 + Z_2 + 4Z_2 = A^2$$

de unde, $Z_1 = I_3 - \frac{1}{2}A^2 + \frac{1}{2}A$, $Z_2 =\frac{1}{3}I_3 + \frac{1}{6}A^2 - \frac{1}{2}A$, $Z_3 =-\frac{1}{3}I_3 +\frac{1}{3}A^2$.

Obținem astfel

$$e^A =(I_3 - \frac{1}{2}A^2 + \frac{1}{2}A)e +(\frac{1}{3}I_3 + \frac{1}{6}A^2 -\frac{1}{2}A)e^{-1} +(-\frac{1}{3}I_3 +\frac{1}{3}A^2)e^2.$$

8. Să se aducă la forma canonică Jordan endomorfismul $u : \mathbf{C}^4 \to \mathbf{C}^4$ căruia îi corespunde transpusa matricei:

$$A = \begin{pmatrix} -3 & 4 & 3 & 8 \\ -4 & 5 & -1 & 4 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 2 & -1 \end{pmatrix}$$

R: Determinăm valorile proprii ale lui A. Avem

$$P_A(\lambda) = \begin{vmatrix} \lambda+3 & -4 & -3 & -8 \\ 4 & \lambda-5 & 1 & -4 \\ 0 & 0 & \lambda-3 & 0 \\ 0 & 0 & -2 & \lambda+1 \end{vmatrix} = (\lambda-1)^2 (\lambda+1) (\lambda-3)$$

Obținem valorile proprii $\lambda_1 = 1$ (cu multiplicitatea algebrică 2) şi $\lambda_2 = -1$ şi $\lambda_3 = 3$. Fie matricea

$$A_1 = A - \lambda_1 I_3 = \begin{pmatrix} -4 & 4 & 3 & 8 \\ -4 & 4 & -1 & 4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix}$$

$$A_1^2 = \begin{pmatrix} 0 & 0 & 6 & -32 \\ 0 & 0 & -10 & -24 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$N_1 = \text{Ker } A_1 = \{(\alpha, \alpha, 0, 0), \alpha \in \mathbf{C}\}$, $\dim_C N_1 = 1$

$N_2 = \text{Ker } A_1^2 = \{(\alpha, \beta, 0, 0), \alpha, \beta \in \mathbf{C}\}$, $\dim_C N_2 = 2$

$F_1 = N_1$, $N_2 = N_1 \oplus F_2$.

$B_1 = \{(0,1,0,0)$ este o bază în $F_2\}$, $e_{11} = (0,1,0,0)$

$e_{21}{}^t = A_1 e_{11}{}^t = (4,4,0,0)$

Deoarece $\dim_C N_1 = 1$, $B_2 = \{e_{21}\}$ este bază în N_1.

Determinăm vectorii proprii asociați valorii proprii λ_2:

$$V_{\lambda_2} = \{(-8\alpha, -6\alpha, 0, \alpha), \alpha \in \mathbf{C}\}$$

Luăm $e'_1 = (-8,-6,0,1)$;

Determinăm subspațiu propriu asociat lui λ_3:

$$V_{\lambda_3} = \{(5\alpha, 11\alpha, -2\alpha, -\alpha), \alpha \in \mathbf{C}\}$$

Luăm $e''_1 = (5,11,-2,-1)$. În baza $B=\{e_{11}, e_{21}, e'_1, e''_3\}$ endomorfismul u are forma canonică

$$J_A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$