SVK Spații vectoriale peste un corp comutativ

Fie K un corp comutativ. Toate conceptele care au fost definite la cursul "Algebră liniară" din sem I, unde K era un subcorp al lui $\mathbb{C}$, pot fi definite identic în cazul în care K este un corp comutativ arbitrar. În particular, conceptele de K-spațiu vectorial, aplicație liniară de spații vectoriale, subspațiu vectorial, subspațiul generat de o mulțime, au exact aceleași definiții. În plus, toate rezultatele pe care le-am demonstrat la cursul de Algebră Liniară pentru K-spații vectoriale, unde K este subcorp al lui $\mathbb{C}$, rămân valabile în cazul în care K este corp comutativ arbitrar.

Fie V un spațiu vectorial peste corpul comutativ K. Reamintim că:

- o mulțime $S \subset V$ se numește <u>sistem de generatori</u> pentru V dacă $\langle S \rangle = V$ (unde $\langle S \rangle$ este subspațiul generat de S); aceasta este echivalent cu faptul că orice $v \in V$ este combinație liniară de un număr finit de elemente ale lui S,
- o mulțime $S \subset V$ se numește <u>liniar independentă</u> dacă pt. orice $n \in \mathbb{N}^*$ și orice $x_1, \ldots, x_n \in S$ distincte și orice $a_1, \ldots, a_n \in K$ cu $a_1 x_1 + \ldots + a_n x_n = 0$, rezultă că $a_1 = \ldots = a_n = 0$.
- o submulțime a lui V se numește <u>bază</u> dacă este sistem de generatori și liniar independentă.

SVK 2

<u>Observație</u>. Dacă $B=(e_i)_{i\in I}$ este o bază a K-spațiului vectorial $V\neq 0$, atunci pt. orice $v\in V$ există $n\in\mathbb{N}^*$, $i_1,\dots,i_n\in I$ distincți și $a_{i_1},\dots,a_{i_n}\in K$ astfel încât

$v=a_{i_1}e_{i_1}+\dots+a_{i_n}e_{i_n}$. Definim $a_i:=0$ pt. orice $i\in I\setminus\{i_1,\dots,i_n\}$ și atunci vom scrie formal că $v=\sum_{i\in I}a_ie_i$. Dacă I este infinită, o astfel de sumă nu are sens (algebric), dar atunci când doar un număr finit de termeni ai sumei sunt $\neq 0$ (așa cum este cazul de față), prin $\sum_{i\in I}a_ie_i$ vom înțelege suma termenilor nenuli ai sumei (sau 0 dacă toți termenii sunt nuli).

Așadar orice $v\in V$ se poate scrie sub forma $v=\sum_{i\in I}a_ie_i$ cu ~~[illegible]~~ $\{i\in I\mid a_i\neq 0\}$ finită. Mai mult, această reprezentare este unică, în sensul că

$$v=\sum_{i\in I}a_ie_i=\sum_{i\in I}b_ie_i \text{ cu } \{i\in I\mid a_i\neq 0\}, \{i\in I\mid b_i\neq 0\}$$

$$\text{finite} \Rightarrow a_i=b_i \text{ pt. orice } i\in I.$$

Într-adevăr, $\sum_{i\in I}a_ie_i=\sum_{i\in I}b_ie_i \Rightarrow$

$\Rightarrow \sum_{i\in I}(a_i-b_i)e_i=0$. Cum B e liniar independentă, trebuie ca $a_i-b_i=0$ pt. orice i, altfel am obține o combinație liniară nulă de un număr finit de e_i-uri diferite și nu toți coeficienții nuli.

Dacă $v=\sum_{i\in I}a_ie_i$, atunci familia $(a_i)_{i\in I}$ reprezintă coordonatele lui v în baza B.

Dacă V este un K-spațiu vectorial, putem pune următoarele întrebări:

1. Are V o bază?

2. Dacă da, ce legătură există între două baze diferite ale lui V?

S-a demonstrat la cursul de Algebră liniară că dacă V este finit generat, atunci V are o bază, și de asemenea că orice două baze ale lui V au același număr de elemente. Vom extinde aceste rezultate la cazul unui spațiu vectorial V arbitrar.

<u>Teoremă</u>. Fie V un spațiu vectorial peste corpul comutativ K. Fie S un sistem de generatori pentru V și F o mulțime liniar independentă cu $F \subset S$. Atunci există o bază B a lui V cu $F \subset B \subset S$.

<u>Demonstrație</u>. Considerăm mulțimea

$$\mathcal{F} = \{ Y \mid F \subset Y \subset S \text{ și } Y \text{ liniar independentă} \}.$$

$\mathcal{F}$ este nevidă, deoarece $F \in \mathcal{F}$. În plus, $\mathcal{F}$ este mulțime ordonată cu relația de incluziune. Arătăm că mulțimea ordonată $(\mathcal{F}, \subseteq)$ este inductiv ordonată. Pentru aceasta, fie $(Y_i)_{i\in I}$ un lanț (submulțime total ordonată) din $\mathcal{F}$ și arătăm că acest lanț are un majorant în $\mathcal{F}$.

Fie $Y = \bigcup_{i\in I} Y_i$. Arătăm că Y este liniar independentă.

Fie $y_1, \ldots, y_n$ distincte în Y, unde $n \in \mathbb{N}^*$. Atunci există $i_1, \ldots, i_n \in I$ cu $y_1 \in Y_{i_1}, \ldots, y_n \in Y_{i_n}$. Cum $(Y_i)_{i\in I}$ este total ordonată (adică pt. orice $i, j \in I$ avem $Y_i \subset Y_j$ sau $Y_j \subset Y_i$), rezultă că una dintre $Y_{i_1}, \ldots, Y_{i_n}$ le include pe toate celelalte (adică este cea mai mare dintre ele în raport cu relația de incluziune); fie de exemplu $Y_{i_1}, \ldots, Y_{i_n} \subset Y_{i_0}$. Atunci $y_1, \ldots, y_n \in Y_{i_0}$ și cum $Y_{i_0} \in \mathcal{F}$, ea este liniar independentă, deci și $\{y_1, \ldots, y_n\}$ este liniar independentă. Rezultă așadar că Y este liniar independentă.

Cum $F \subset Y_i \subset S$ pentru orice $i \in I$, este clar că $F \subset Y \subset S$, de unde $Y \in \mathcal{F}$. În plus, $Y_i \subset Y$ pentru orice $i \in I$, adică Y este un majorant în $\mathcal{F}$ pentru lanțul $(Y_i)_{i\in I}$.

Am arătat deci că orice lanț din $\mathcal{F}$ are un majorant în $\mathcal{F}$. Putem atunci aplica Lema lui Zorn și rezultă că $\mathcal{F}$ are un element maximal B. Așadar $F \subset B \subset S$ și B este liniar independent. Arătăm că B este și sistem de generatori, de unde va rezulta că B este o bază așa cum dorim și demonstrația va fi încheiată.

Este suficient să arătăm că $S \subset \langle B \rangle$, de unde va rezulta că și B este sistem de generatori. Într-adevăr, dacă nu ar fi așa, atunci fie $s \in S \setminus \langle B \rangle$.

Atunci $B \cup \{s\}$ este liniar independentă, deoarece dacă $z_1, \dots, z_n \in B \cup \{s\}$ sunt distincte și $a_1 z_1 + \dots + a_n z_n = 0$, unde $a_1, \dots, a_n \in K$, atunci:

- dacă niciunul dintre $z_1, \dots, z_n$ nu este s, atunci $z_1, \dots, z_n \in B$, și cum B e lin. indep. $\Rightarrow a_1 = \dots = a_n = 0$.
- dacă unul dintre $z_1, \dots, z_n$ este s, fie de exemplu $z_n = s$, atunci $a_n s = a_n z_n = -a_1 z_1 - \dots - a_{n-1} z_{n-1}$. Dacă $a_n \neq 0$ ar rezulta că $s = -a_n^{-1} a_1 z_1 - \dots - a_n^{-1} a_{n-1} z_{n-1} \in \langle B \rangle$ (deoarece $z_1, \dots, z_{n-1} \in B$), contradicție. Așadar $a_n = 0$ și atunci $a_1 z_1 + \dots + a_{n-1} z_{n-1} = 0$ arată că și $a_1 = \dots = a_{n-1} = 0$ (B fiind lin. indep.).

Cum $F \subset B \cup \{s\} \subset S$, obținem că $B \cup \{s\} \in \mathcal{F}$. Dar $B \subsetneq B \cup \{s\}$, ceea ce contrazice faptul că B este element maximal al lui $\mathcal{F}$. Contradicția obținută arată că $S \subset \langle B \rangle$ și demonstrația este încheiată.

Corolar. Fie V un K-spațiu vectorial, unde K este corp comutativ. Atunci:

(i) Dacă F este liniar independentă în V, atunci există o bază B a lui V cu $F \subset B$.

(ii) Dacă S este sistem de generatori în V, atunci există o bază B a lui V cu $B \subset S$.

SVK 6

<u>Demonstrație</u>. (i) Aplicăm Teorema pt. $S = V$.

(ii) Aplicăm Teorema pt. $F = \phi$.

<u>Corolar</u>. Orice spațiu vectorial V peste un corp comutativ are o bază.

<u>Dem</u>. Rezultă direct din Corolarul precedent, (ii), pt. $S = V$.

Dăm acum un răspuns celei de-a doua întrebări.

<u>Teoremă</u>. Fie V un spațiu vectorial peste corpul comutativ K și fie B_1, B_2 două baze ale lui V. Atunci există o bijecție între B_1 și B_2 (adică B_1 și B_2 au același cardinal).

<u>Demonstrație</u>. S-a demonstrat la cursul de "Algebră liniară" că dacă una dintre B_1 și B_2 este finită (deci V este finit generat), atunci orice bază este finită și orice două baze au același număr de elemente, deci sunt în bijecție. (demonstrația a folosit Teorema schimbului).

Rămâne de demonstrat în situația în care B_1 și B_2 sunt infinite. Fie $B_1 = \{x_i \mid i \in I\}$ și $B_2 = \{y_j \mid j \in J\}$.

Pentru fiecare $i \in I$, x_i este o combinație liniară de câteva (un număr finit) de elemente din B_2, deci există F_i finită, $F_i \subset J$ cu $x_i \in \langle y_j \mid j \in F_i \rangle$.

Arătăm că $\bigcup_{i \in I} F_i = J$. Într-adevăr, dacă ar exista $j_0 \in J \setminus \bigcup_{i \in I} F_i$, atunci pentru orice $i \in I$ avem $j_0 \notin F_i$, deci $x_i \in \langle y_j \mid j \in J \setminus \{j_0\} \rangle$. Cum B_1 este sistem de generatori pt. V, rezultă că și $\{y_j \mid j \in J \setminus \{j_0\}\}$ este.

În particular $y_{j_0} \in \langle y_j \mid j \in J \setminus \{j_0\} \rangle$, deci există $n \in \mathbb{N}^*$, $j_1, \dots, j_n \in J \setminus \{j_0\}$ și $a_1, \dots, a_n \in K$ cu

$y_{j_0} = a_1 y_{j_1} + \dots + a_n y_{j_n}$. Cum $j_0 \neq j_1, \dots, j_n$, aceasta contrazice liniar independența lui B_2.

Așadar $\bigcup_{i \in I} F_i = J$. Acum orice F_i este finită, deci $|F_i| < \aleph_0$ (unde $\aleph_0 = |\mathbb{N}|$). Rezultă că

$$|J| = |\bigcup_{i \in I} F_i| \leq |I| \cdot \aleph_0 .$$

Dar I este infinită, deci $\aleph_0 \leq |I|$, și în plus

$|I| \cdot \aleph_0 = |I|$ (a se vedea cursul de "Logică și teoria mulțimilor" pentru detalii).

Obținem că $|J| \leq |I|$.

Procedând similar (schimbând rolurile lui B_1 și B_2 în discuția de mai sus), obținem $|I| \leq |J|$.

Din Teorema Cantor-Bernstein obținem că $|I| = |J|$, deci $|B_1| = |B_2|$.

<u>Consecință</u>. Putem acum defini dimensiunea unui spațiu vectorial ca fiind cardinalul unei baze.
(Dimensiunea este un număr cardinal).

Polinomul minimal al unei transformări liniare

Fie V un spațiu vectorial de dimensiune finită peste corpul comutativ K și fie $T:V\to V$ o aplicație liniară ($\Leftrightarrow$ transformare liniară).

Dacă $f\in K[X]$, $f=a_sX^s+\dots+a_1X+a_0$, definim

$$f(T)\stackrel{def.}{=}a_sT^s+\dots+a_1T+a_01_V\in End_K(V)$$

(unde $1_V:V\to V$ este aplicația identitate).

Dacă $f,g\in K[X]$ se verifică imediat că

$$(f+g)(T)=f(T)+g(T) \text{ și } (fg)(T)=f(T)g(T).$$

(Atenție: înmulțirea în $End_K(V)$ este compunerea, deci $T^i=\underbrace{T\circ\dots\circ T}_{i \text{ ori}}$, $f(T)g(T)=f(T)\circ g(T)$, etc.).

Fie acum $I=\{f\in K[X]\mid f(T)=0\}$, care este clar ideal în $K[X]$. Cum $1_V, T, T^2,\dots\in End_K(V)$, iar $End_K(V)\simeq M_n(K)$, izomorfism de K-spații vectoriale, unde $n=\dim_K V$, obținem că $\{1_V, T, T^2,\dots\}$ este liniar dependentă, deci există $s\in\mathbb{N}^*$ și $a_0,\dots,a_s\in K$, nu toate nule, cu $a_01_V+a_1T+\dots+a_sT^s=0$, deci există $f\in K[X]$, $f\neq 0$, cu $f(T)=0$. Prin urmare $I\neq 0$ și cum orice ideal în $K[X]$ este principal, există un unic polinom monic $\mu_T \in K[X]$ cu $I = (\mu_T)$. Acest μ_T se numește polinomul minimal al lui T. Avem deci

μ_T este polinomul minimal al lui T $\Leftrightarrow$ $\begin{cases} \cdot\ \mu_T \in K[X] \text{ este monic} \\ \cdot\ \mu_T(T) = 0 \\ \cdot\ \text{Dacă } f \in K[X] \text{ și } f(T) = 0 \Rightarrow \mu_T \mid f \end{cases}$

Exercițiu. μ_T se poate defini echivalent ca fiind polinomul monic de grad minim posibil cu $\mu_T(T) = 0$.

Propoziție. Fie $T: V \to V$ transformare liniară și $V_1, \dots, V_r$ subspații (nenule) T-invariante ale lui V astfel încât $V = V_1 \oplus \dots \oplus V_r$. Fie $T_i = T_{|V_i} \in End_K(V_i)$ și μ_i polinomul minimal al lui T_i. Atunci

$$\mu_T = c.m.m.m.c(\mu_1, \dots, \mu_r).$$

Demonstrație. Notăm $\mu = c.m.m.m.c(\mu_1, \dots, \mu_r)$.

Fie $x \in V_i$, unde $1 \le i \le r$. Atunci $\mu(T)(x) = \mu(T_i)(x)$.

Dar $\mu_i \mid \mu$, deci $\mu(T_i) = 0$ și atunci $\mu(T_i)(x) = 0$.

Obținem că $\mu(T)(x) = 0$, deci $\mu(T)(V_i) = 0$ pentru orice i, de unde $\mu(T) = 0$. Aceasta arată că $\mu_T \mid \mu$.

Pe de altă parte, $\mu_T(T) = 0 \Rightarrow \mu_T(T_{|V_i}) = 0$, adică $\mu_T(T_i) = 0$ pt. orice i. Atunci $\mu_i \mid \mu_T$ pentru orice i, deci și $\mu = c.m.m.m.c(\mu_1, \dots, \mu_r) \mid \mu_T$. Rezultă că $\mu = \mu_T$.

Lemă. Fie V un K-spațiu vectorial de dimensiune $n \in \mathbb{N}^*$. Dacă $T : V \to V$ este o transformare liniară pentru care există o bază B a lui V cu $M_B(T) = J_n(\lambda)$ pentru un $\lambda \in K$

(unde $M_B(T)$ este matricea lui T în baza B, iar $J_n(\lambda)$ este celula Jordan de tip $n \times n$ asociată lui λ),

atunci $\mu_T = (X-\lambda)^n$.

Dem. ~~Notăm N~~ Dacă $n=1$, deci $M_B(T) = J_1(\lambda) = (\lambda)$, atunci $T = \lambda 1_V$ și e clar că $\mu_T = X - \lambda$.

Fie $n \geq 2$. Notăm

$$N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ & 0 & 1 & 0 & \vdots \\ & & 0 & \ddots & 0 \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix} \in M_n(K).$$

Avem $M_B(T) = J_n(\lambda) = \lambda I_n + N$. Atunci

$M_B(T - \lambda 1_V) = M_B(T) - \lambda M_B(1_V) = \lambda I_n + N - \lambda I_n = N$.

Un calcul direct arată că $N^{n-1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & & 0 \end{pmatrix} \neq 0$ și $N^n = 0$.

Așadar $M_B((T-\lambda 1_V)^n) = N^n = 0$, deci $f(T) = 0$, unde $f = (X-\lambda)^n$. Obținem că $\mu_T \mid f$, de unde $\mu_T = (X-\lambda)^m$ pentru un $m \leq n$. Dacă $m < n$, atunci

$M_B((T-\lambda 1_V)^m) = N^m \neq 0$, deci $(T-\lambda 1_V)^m \neq 0$, contradicție.

Rămâne că $m = n$, deci $\mu_T = (X-\lambda)^n$.

SVK 11

<u>Teoremă</u>. Fie V un K-spațiu vectorial nenul finit dimensional, unde K este corp comutativ, și fie $T: V \to V$ o transformare liniară astfel încât polinomul caracteristic P_T al lui T este produs de factori liniari în $K[X]$. Fie $\lambda_1, \dots, \lambda_r$ valorile proprii distincte ale lui T și pentru fiecare $1 \le i \le r$ fie m_i dimensiunea maximă a unei celule Jordan asociate lui λ_i în forma canonică Jordan a lui T ($\iff m_i$ este indicele de nilpotență al transformării liniare $(T - \lambda_i 1_V)_{|V^{\lambda_i}(T)}$, cu notațiile de la cursul de Algebră liniară).

Atunci $\mu_T = (X-\lambda_1)^{m_1} \cdot \ldots \cdot (X-\lambda_r)^{m_r}$.

<u>Demonstrație</u>. Știm că $V = V_1 \oplus \ldots \oplus V_r$, unde $V_i = V^{\lambda_i}(T)$.

În plus, pt. fiecare $1 \le i \le r$, V_i este sumă directă de spații ciclice relativ la $(T - \lambda_i 1_V)_{|V_i}$, fiecare astfel de ~~o bază în care~~ spațiu ciclic U având o bază în care matricea lui $T_{|U}$ este $J_h(\lambda)$ pt. un $h \le m_i$; mai mult, pt. unul dintre aceste U matricea este chiar $J_{m_i}(\lambda)$. Din Lema precedentă și Propoziția anterioară rezultă că polinomul minimal al lui $T_{|V_i}$ este $(X-\lambda_i)^{m_i}$, iar apoi polinomul minimal al lui T este

$$\text{c.m.m.m.c}\left((X-\lambda_1)^{m_1}, \dots, (X-\lambda_r)^{m_r}\right) = (X-\lambda_1)^{m_1} \cdot \ldots \cdot (X-\lambda_r)^{m_r}.$$

<u>Corolar</u>. Dacă $T: V \to V$ și P_T este produs de factori liniari în $K[X]$, atunci $P_T(T) = 0$.

<u>Demonstrație</u>. Cu notațiile din Teorema precedentă avem $\mu_T = (X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}$, iar $P_T = (X-\lambda_1)^{a_1} \cdots (X-\lambda_r)^{a_r}$, unde a_i este multiplicitatea algebrică a lui λ_i ($\Leftrightarrow a_i = \dim V^{\lambda_i}(T)$).
Dar $m_i \leq a_i$ pt. orice i, deci $\mu_T \mid P_T$.
Rezultă atunci că $P_T(T) = 0$.

<u>Teoremă</u> (Cayley-Hamilton) Fie K un corp comutativ, $n \in \mathbb{N}^*$ și $A \in M_n(K)$. Atunci $P_A(A) = 0$, unde P_A este polinomul caracteristic al lui A.

<u>Demonstrație</u>. Presupunem mai întâi că P_A este produs de factori liniari în $K[X]$. Fie V un K-spațiu vectorial de dimensiune n, fie B o bază a lui V și $T: V \to V$ transformarea liniară pt. care $M_B(T) = A$. Atunci $P_A = \det(XI_n - A) = P_T$. Din corolarul precedent știm că $P_T(T) = 0$, de unde $P_T(A) = 0$, adică $P_A(A) = 0$.
Considerăm acum situația generală, în care P_A nu mai este neapărat produs de factori liniari în $K[X]$. Am demonstrat însă că există o extindere de corpuri $K \subset E$ astfel încât P_A are toate rădăcinile în E,

SVK 13

altfel spus, P_A este produs de factori liniari din $E[X]$.

Cum $M_n(K) \subset M_n(E)$, putem privi A în $M_n(E)$.

Evident, P_A este același când o privim astfel, și atunci aplicând cazul inițial (deoarece P_A e produs de factori liniari din $E[X]$), obținem că $P_A(A)=0$.

Corolar. Pentru orice transformare liniară $T: V \to V$, unde V este un K-spațiu vectorial nenul finit dimensional, avem $P_T(T)=0$.