

Leçon 151. Dimension d'un espace vectoriel (de dimension finie). Rang. Exemples et applications.

Devs :

- Critère de Kalman
- Théorème de Gauss Wantzel

Références :

1. Griffone, Algèbre linéaire
2. Perrin, Cours d'Algèbre
3. Caldero, H2G2
4. Gozard, Théorie de Galois
5. Carrega, Théorie des corps
6. Coron, Contron and nonlinearity

1 Théorie de la dimension

On se donne un espace vectoriel E sur un corps commutatif K .

1.1 Familles libres, génératrices et bases

Définition 1. Une famille de vecteurs (v_1, \dots, v_p) de E est dite *génératrice* si $E = \text{Vect}(v_1, \dots, v_p)$, ce qui signifie que pour tout $x \in E$, il existe $(\lambda_1, \dots, \lambda_p) \in K^p$ tel que $x = \lambda_1 v_1 + \dots + \lambda_p v_p$.

Exemple 2. Dans \mathbb{R}^2 , la famille (v_1, v_2) donnée par $v_1 = (1, 1)$ et $v_2 = (1, -1)$ est génératrice. Dans $\mathbb{R}[X]$, il n'existe pas de famille génératrice finie.

Définition 3. Soit (v_1, \dots, v_p) une famille finie d'éléments de E . On dit qu'elle est *libre* si pour tout $(\lambda_1, \dots, \lambda_p) \in K^p$ tel que $\lambda_1 v_1 + \dots + \lambda_p v_p = 0$, on a $\lambda_1 = \dots = \lambda_p = 0$. On dit qu'elle est *liée* si elle n'est pas libre.

Proposition 4. Une famille (v_1, \dots, v_p) est liée si et seulement si un des vecteurs v_i s'écrit comme combinaison linéaire des autres vecteurs.

Proposition 5. Soit (v_1, \dots, v_p) une famille libre d'éléments de E , et $x \in \text{Vect}(v_1, \dots, v_p)$. Alors la décomposition de x sur les v_i est unique.

Définition 6. On appelle *base* de E une famille à la fois libre et génératrice.

Proposition 7. Une famille (v_1, \dots, v_p) de E est une base si et seulement si tout élément $x \in E$ se décompose de manière unique sur les v_i .

Exemple 8. La famille $((1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1))$ est une base de K^n , appelée la base canonique de K^n .

Proposition 9. On a les propriétés suivantes :

- $\{x\}$ est une famille libre $\iff x \neq 0$.
- Toute famille contenant une famille génératrice est génératrice.
- Toute sous-famille d'une famille libre est libre.
- Toute famille contenant une famille liée est liée.
- Toute famille (v_1, \dots, v_p) dont l'un des v_i est nul, est liée.

1.2 Espaces et sous espaces vectoriels de dimension finie

Définition 10. On dit que E est de *dimension finie* si il admet une famille génératrice finie. Dans le cas contraire, on dit qu'il est de *dimension infinie*.

Théorème 11. (De la base incomplète). Soit $E \neq \{0\}$ un espace vectoriel de dimension finie, et \mathcal{G} une famille génératrice de E . Considérons une famille libre $\mathcal{L} \subset \mathcal{G}$. Il existe une base \mathcal{B} telle que $\mathcal{L} \subset \mathcal{B} \subset \mathcal{G}$.

Corollaire 12. Si $E \neq \{0\}$ est un espace vectoriel de dimension finie, alors de toute famille génératrice finie, on peut extraire une base, et toute famille libre peut être complétée en une base de E .

Lemme 13. (Lemme de Steinitz). Dans un espace vectoriel engendré par n éléments, toute famille contenant plus de n éléments est liée.

Théorème 14. Dans un espace vectoriel E de dimension finie, toutes les bases ont le même nombre d'éléments. Ce nombre est appelé la *dimension* de E sur K , et est noté $\dim_K(E)$ ou $\dim(E)$ s'il n'y a pas d'ambiguïté.

Théorème 15. Soit E un espace vectoriel de dimension n . Alors toute famille génératrice ayant n éléments est une base, et toute famille libre ayant n éléments est une base.

Proposition 16. Soit E un espace vectoriel de dimension finie et F un sous-espace vectoriel de E . Alors F est de dimension finie et $\dim(F) \leq \dim(E)$. De plus, on a $\dim(F) = \dim(E) \iff F = E$.

On suppose dorénavant que E est de dimension finie.

Définition 17. Soit E_1, E_2 des sous-espaces vectoriels de E . On appelle somme de E_1 et E_2 le sous-espace de E défini par $E_1 + E_2 = \{x_1 + x_2 : x_1 \in E_1 \text{ et } x_2 \in E_2\}$.

Proposition 18. Soit E_1, E_2 des sous-espaces vectoriels de E , et $\mathcal{E} = E_1 + E_2$. La décomposition de tout élément de \mathcal{E} en somme d'un élément de E_1 et d'un élément de E_2 est unique, si et seulement si $E_1 \cap E_2 = \{0\}$. On écrit alors $\mathcal{E} = E_1 \oplus E_2$ et on dit que E_1 et E_2 sont en somme directe, ou supplémentaires.

Proposition 19. Soit E_1, E_2 des sous-espaces vectoriels de E . Alors $E = E_1 \oplus E_2$ si et seulement si pour toute base \mathcal{B}_1 de E_1 et toute base \mathcal{B}_2 de E_2 , $\{\mathcal{B}_1, \mathcal{B}_2\}$ est une base de E . On dit que $\{\mathcal{B}_1, \mathcal{B}_2\}$ est une base adaptée à la décomposition $E = E_1 \oplus E_2$.

Proposition 20. (Formule de Grassman). Soit E_1, E_2 deux sous-espaces vectoriels de E . Alors

$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2).$$

En particulier, $\dim(E_1 \oplus E_2) = \dim(E_1) + \dim(E_2)$.

Proposition 21. Tout sous-espace vectoriel de E admet un supplémentaire, et tous ses supplémentaires sont de même dimension.

1.3 Dimension et applications linéaires

On se donne E et F deux espaces vectoriels de dimension finie et $f \in \mathcal{L}(E, F)$.

Proposition 22.

- Si f est injective et que la famille (v_1, \dots, v_p) est libre, alors $(f(v_1), \dots, f(v_p))$ est libre.
- Si f est surjective et que la famille (v_1, \dots, v_p) est génératrice, alors $(f(v_1), \dots, f(v_p))$ est génératrice.
- Si f est bijective et que la famille (v_1, \dots, v_p) est une base, alors $(f(v_1), \dots, f(v_p))$ est une base.

Proposition 23. Deux espaces vectoriels de dimension finie sont isomorphes si et seulement si ils ont la même dimension.

Proposition 24. L'espace $\mathcal{L}(E, F)$ est de dimension finie et $\dim \mathcal{L}(E, F) = \dim(E) \times \dim(F)$.

2 Rang. Applications

On se donne E et F deux espaces vectoriels de dimension finie.

2.1 Rang d'une application linéaire

Définition 25. Soit $f \in \mathcal{L}(E, F)$. Alors $f(E)$ est un sous-espace vectoriel de F , et on appelle rang de f sa dimension. On note ainsi $\text{rg}(f) = \dim(f(E))$.

Théorème 26. (Théorème du rang). Soit $f \in \mathcal{L}(E, F)$. On a $\dim(E) = \text{rg}(f) + \dim(\text{Ker } f)$. En particulier, $E/\text{Ker}(f) \simeq \text{Im}(f)$.

Exemple 27. Si $p \in \mathcal{L}(E)$ est un projecteur, on a $\text{Ker}(f) \oplus \text{Im}(f) = E$. Ce résultat est cependant faux pour un endomorphisme quelconque.

Corollaire 28. Soit $f \in \mathcal{L}(E, F)$. On suppose que $\dim(E) = \dim(F)$. Alors les propriétés suivantes sont équivalentes :

1. f est injective.
2. f est surjective.
3. f est bijective.

Remarque 29. Ce résultat n'est pas vrai en dimension infinie. L'application dérivation sur $\mathbb{R}[X]$, qui à P associe P' , est surjective mais pas injective.

2.2 Rang d'une matrice

On se donne $n, p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,p}(K)$.

Définition 30. On appelle rang de A le rang de la famille des vecteurs colonnes de A . Si $A = (C_1 \mid \dots \mid C_n)$, on définit ainsi $\text{rg}(A) = \dim \text{Vect}(C_1, \dots, C_n)$.

Proposition 31. Soit E et F deux espaces vectoriels de dimension finie et $f \in \mathcal{L}(E, F)$. Soit $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (f_1, \dots, f_p)$ des bases respectives de E et de F , et $A = \text{mat}_{\mathcal{B}, \mathcal{B}'}(f)$. Alors $\text{rg}(f) = \text{rg}(A)$.

Proposition 32. Pour toute matrice $A \in \mathcal{M}_{n,p}(K)$, $\text{rg}(A) = \text{rg}(A^T)$.

Définition 33. (Action de Steinütz)

$\text{GL}_n(K) \times \text{GL}_p(K)$ agit sur $\mathcal{M}_{n,p}(K)$ par équivalence, via :

$$\begin{cases} (\text{GL}_n(K) \times \text{GL}_p(K)) \times \mathcal{M}_{n,p}(K) & \rightarrow \mathcal{M}_{n,p}(K) \\ ((P, Q), M) & \mapsto PMQ^{-1} \end{cases}$$

Proposition 34. (Théorème du rang, reformulation matricielle).

Chaque orbite pour cette action contient un représentant de la forme :

$$A = \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix},$$

où k est le rang de la matrice A .

Remarque 35. La méthode du pivot de Gauss permet, pour une matrice $A \in \mathcal{M}_{n,p}(K)$ donnée, de déterminer un représentant de la forme $\begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$ en échelonnant A grâce à des opérations élémentaires sur ses colonnes, ou sur ses lignes. Cela fournit donc un moyen pratique de calculer le rang de A .

Remarque 36. Deux matrices carrées semblables sont équivalentes. La réciproque n'est pas vraie en générale, par exemple $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ sont équivalentes, car de rang 1 mais pas semblables, car leur trace est différente.

2.3 Application : un critère de contrôlabilité pour les EDO

On se donne un intervalle $]T_0, T_1[$ de \mathbb{R} , et on considère problème de Cauchy :

$$(\mathcal{P}_0): \begin{cases} x'(t) = A(t)x(t) + B(t)u(t) \\ x(T_0) = x_0 \end{cases}$$

avec $A \in L^\infty(]T_0, T_1[, \mathcal{M}_n(\mathbb{R}))$, $B \in L^\infty(]T_0, T_1[, \mathcal{M}_{m,n}(\mathbb{R}))$ et $u \in L^\infty(]T_0, T_1[, \mathbb{R}^m)$ et $x_0 \in \mathbb{R}^n$.

Définition 37.

On dit que le système $x'(t) = A(t)x(t) + B(t)u(t)$ est contrôlable si pour tout $(x_0, x_1) \in \mathbb{R}^n \times \mathbb{R}^n$, il existe $u \in L^\infty(]T_0, T_1[, \mathbb{R}^m)$ tel que la solution $x \in \mathcal{C}^0(]T_0, T_1[, \mathbb{R}^n)$ du problème de Cauchy (\mathcal{P}_0) vérifie $x(T_0) = x_0$ et $x(T_1) = x_1$.

Définition 38. On définit le Gramian de contrôlabilité du système $x'(t) = A(t)x(t) + B(t)u(t)$ comme la matrice $\mathfrak{C} \in \mathcal{S}_n(\mathbb{R})$ vérifiant

$$\mathfrak{C} := \int_{T_0}^{T_1} R(T_1, s) B(s) B(s)^T R(T_1, s)^T ds,$$

où M^T signifie la transposée de M .

Théorème 39. Le système de contrôle $x'(t) = A(t)x(t) + B(t)u(t)$ est contrôlable si et seulement si son Gramian de contrôle \mathfrak{C} est inversible.

Exemple 40. Le système de contrôle $\begin{cases} x'_1(t) = u \\ x'_2(t) = x_1(t) + tu \end{cases}$ où $u \in \mathbb{R}$ et $t \in [0, T]$ avec

$T > 0$ a pour Gramian de contrôlabilité $\mathfrak{C} = \begin{pmatrix} T & T^2 \\ T^2 & T^3 \end{pmatrix}$, qui est de rang 1. On en déduit que ce système est contrôlable.

Développement 1 :

Théorème 41. (Condition de Kalman)

On suppose que A, B et u ne dépendent pas du temps. Alors le système de contrôle $x'(t) = Ax(t) + Bu$ est contrôlable sur $[T_0, T_1]$ si et seulement si $\text{Vect}(A^i B u : u \in \mathbb{R}^m \text{ et } i \in \{0, \dots, n-1\}) = \mathbb{R}^n$, c'est-à-dire si et seulement si le rang de la matrice $(A^0 B \mid \dots \mid A^{n-1} B)$ est égal à n .

3 Dimension en théorie des corps

3.1 Extensions de corps et base télescopique

Définition 42. Soit K un corps. On appelle extension de K tout corps L tel qu'il existe un morphisme de corps j de K dans L . On note L/K pour dire que L est une extension de K .

Remarque 43. L est une extension de K ssi K peut être vu (à isomorphisme près) comme un sous-corps de L .

Exemple 44. \mathbb{C} est une extension de \mathbb{R} lui-même extension de \mathbb{Q} .

Exemple 45. Tout corps K est une extension de son sous-corps premier P .

Définition 46. Soit K un corps et L/K une extension. On appelle degré de L/K et on note $[L:K]$ la dimension de L vu comme K -espace vectoriel : $[L:K] := \dim_K(L)$.

Théorème 47. (Base télescopique)

Soit $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une base de L sur K , $(f_j)_{j \in J}$ une base de M sur L . Alors $(e_i f_j)_{i \in I, j \in J}$ est une base de M sur K . En particulier, $[M:K] = [M:L][L:K]$.

3.2 Elements et extensions algébriques

Définition 48. Soit L/K une extension, et $A \subset L$. On dit que A engendre L , et on écrit $L = K(A)$ si L est le plus petit sous-corps de L contenant A et K . Si A est fini et $A = \{\alpha_1, \dots, \alpha_n\}$, on note $L = K(\alpha_1, \dots, \alpha_n)$.

Définition 49. Soit K un corps et L une extension de K . Soit $\varphi: K[T] \rightarrow L$ l'homomorphisme défini par $\varphi|_K = \text{id}_K$ et $\varphi(T) = \alpha$.

Si φ est injectif, on dit que α est transcendant sur K . Sinon, on dit que α est algébrique sur K , et l'idéal $I = \text{Ker } \varphi$ étant principal, on a $I = (P)$ avec P irréductible (que l'on peut supposer unitaire). Le polynôme P est, par définition, le polynôme minimal de α sur K , et on le note μ_α .

Exemple 50. $\sqrt{2}$ et i sont algébriques sur \mathbb{Q} , mais pas π ni e .

Remarque 51. Le polynôme minimal d'un élément α algébrique sur K est l'unique polynôme unitaire irréductible de $K[X]$ qui annule α .

Exemple 52. $X^2 + 1$ est le polynôme minimal de i sur \mathbb{Q} . $X - i$ est le polynôme minimal de i sur \mathbb{C} .

Théorème 53. Soit $K \subset L$ une extension et $\alpha \in L$. Les propriétés suivantes sont équivalentes :

- α est algébrique sur K
- On a $K[\alpha] = K(\alpha)$
- On a $\dim_K K[\alpha] < \infty$

Dans ce cas, on a $\deg(\mu_\alpha) = [K(\alpha) : K]$.

Définition 54. Une extension L/K est dite finie si on a $[L : K] < \infty$. Elle est dite algébrique si tous les éléments de L sont algébriques sur K .

Remarque 55. Une extension finie est toujours algébrique, mais la réciproque est fautive, par exemple $\mathbb{Q}\left[\sqrt{\frac{1}{2^n}}, n \in \mathbb{N}^*\right]$ est algébrique et infinie.

Théorème 56. Soit L/K une extension. Alors $M := \{x \in L : x \text{ est algébrique sur } K\}$ est un sous-corps de L .

3.3 Nombres constructibles

Définition 57. On dit qu'un nombre réel est constructible si c'est une des coordonnées d'un point constructible (à la règle non graduée et au compas).

Théorème 58. (Wantzel, 1837). Tout nombre constructible est algébrique sur \mathbb{Q} et son degré est une puissance de 2.

Définition 59. Soit $\theta \in \mathbb{R}$. On note $\hat{\theta}$ l'angle orienté dont une mesure en radian est θ . L'angle $\hat{\theta}$ est dit constructible si le point M du cercle de centre $O = (0, 0)$ et de rayon 1 tel que $(\vec{OI}, \vec{OM}) = \hat{\theta}$, où $I = (1, 0)$, est un point constructible.

Proposition 60. L'angle $\hat{\theta}$ est constructible si et seulement si le réel $\cos(\theta)$ est constructible.

Lemme 61.

1. Les angles de la forme $\frac{\hat{2}\pi}{2^\alpha}$ sont constructibles pour $\alpha \in \mathbb{N}$.
2. Soient $n, m \in \mathbb{N}^*$ premiers entre eux. Alors l'angle $\frac{\hat{2}\pi}{mn}$ est constructible si et seulement si les angles $\frac{\hat{2}\pi}{m}$ et $\frac{\hat{2}\pi}{n}$ le sont.

Développement 2 :

Théorème 62. (Gauss-Wantzel)

Soit p un nombre premier impair, et $\alpha \in \mathbb{N}^*$. Alors l'angle $\frac{\hat{2}\pi}{p^\alpha}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat, c'est-à-dire $p = 1 + 2^{2^\beta}$ pour un certain $\beta \in \mathbb{N}$.