151 — Dimension d'un espace vectoriel (en dimension finie), rang. Exemples et applications.

Soit $\mathbb{K}$ corps et E un $\mathbb{K}$-espace vectoriel ~~de dimension~~ $n \in \mathbb{N}$, E' un autre $\mathbb{K}$-espace vectoriel.

I] Dimension d'un espace vectoriel

1] Notion de dimension et complétion de base

[Gri] I.4

Définitions 1 : Une famille de vecteurs $\{v_1;\dots;v_p\} \in E$ est génératrice si $E = \mathrm{Vect}(v_1;\dots;v_p)$. E est dit de dimension finie s'il existe une famille génératrice finie. Une famille de vecteurs $\{v_1;\dots;v_p\}$ est libre si $\lambda_1 v_1 + \dots + \lambda_p v_p = 0 \Rightarrow \lambda_1 = \dots = \lambda_p = 0$. On appelle base une famille à la fois libre et génératrice.

Proposition 2 : Soit $\mathfrak{B} = (v_i)_{i=1}^n$ base de E.
Alors : l'application $\varphi_{\mathfrak{B}} : E \to \mathbb{K}^n$, $x = x_1 v_1 + \dots + x_n v_n \mapsto (x_1;\dots;x_n)$ est bijective.

Exemples 3 : (1) La base $(e_k = (0;\dots;0;1;0;\dots;0))_{k=1}^n$ (1 en k-ième position) de E est appelée base canonique de $\mathbb{K}^n$.
(2) La base canonique de $\mathbb{R}_n[X]$ est : $(X^k)_{k=0}^n$.

Théorème 4 : Soit G famille génératrice de E, et $L \subseteq G$ une famille libre.
Alors : il existe une base $\mathfrak{B}$ de E telle que $L \subseteq \mathfrak{B} \subseteq G$.

Corollaire 5 : De toute famille génératrice on peut extraire une base.

Théorème 6 : (de la base incomplète) Toute famille libre peut être complétée de manière à former une base.

Lemme 7 : Soit E engendré par n éléments.
Alors : toute famille contenant plus de n éléments est liée.

Théorème 8 : Toutes les bases ont même nombre d'éléments.

Corollaire 9 : (1) Toute famille ayant plus de n éléments est liée.
(2) Toute famille ayant moins de n éléments n'est pas génératrice.

2] Dualité en dimension finie

[Gri] III.3

Définition 10 : On appelle forme linéaire sur E toute application linéaire $f : E \to \mathbb{K}$. On note leur ensemble $\mathcal{L}_{\mathbb{K}}(E;\mathbb{K}) = E^*$ l'espace dual de E.

[Gri] III.8

Proposition 11 : Soit $f \in E^* \setminus \{0\}$.
Alors : $\dim(\ker(f)) = n-1$ i.e. $\ker(f)$ est un hyperplan de E.

Proposition 12 : $\dim(E) = \dim(E^*)$

Théorème 13 : Soit $(e_i)_{i=1}^n$ base de E.
Alors $\left(e_i^*(e_j) := \delta_{i,j} = \begin{cases} 1 & \text{si } i=j \\ 0 & \text{sinon} \end{cases}\right)_{i=1}^n$ est une base de E^*.
On appelle cette base, base duale de $(e_i)_{i=1}^n$.

Exemple 14 : Soit $e_1 = \begin{pmatrix}1\\1\\1\end{pmatrix}$; $e_2 = \begin{pmatrix}1\\0\\-1\end{pmatrix}$ et $e_3 = \begin{pmatrix}0\\1\\1\end{pmatrix}$. La base duale de $(e_1;e_2;e_3)$ est : $(f_1(x) = x_1 - x_2 + x_3$; $f_2(x) = x_2 - x_3$; $f_3(x) = -x_1 + 2x_2 - x_3)$.

Définition 15 : Le bidual de E est : $E^{**} := (E^*)^* = \mathcal{L}_{\mathbb{K}}(E^*;\mathbb{K})$

Proposition 16 : E^{**} est canoniquement isomorphe à E^*.

3] Application de la notion de dimension à la réduction

[Rom] XXII.10

Définition 17 : Soit E un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire $\langle \cdot | \cdot \rangle$. Un endomorphisme $u \in \mathcal{L}(E)$ est dit normal si $u^* \circ u = u \circ u^*$.

Exemple 18 : $S(E)$; $A(E)$; $O(E)$ sont des ensembles d'endomorphismes normaux.

Lemme 19 : Soit $u \in \mathcal{L}(E)$ normal et F sous-espace stable par u.
Alors : $F^\perp$ est stable par u.

Lemme 20 : Soit $u \in \mathcal{L}(E)$.
Alors : il existe un sous-espace vectoriel P de E de dimension 1 ou 2 stable par u.

Lemme 21 : Soit $u \in \mathcal{L}(E)$ endomorphisme normal.
Alors : il existe des sous-espaces vectoriels de E : $P_1;\dots;P_r$ de dimensions 1 ou 2, deux à deux orthogonaux, stables par u tels que $E = \bigoplus_{j=1}^r P_j$.

Théorème 22 : Soit $u \in \mathcal{L}(E)$ endomorphisme normal.
Alors : il existe une base $\mathfrak{B}$ de E telle que $\mathrm{Mat}_{\mathfrak{B}}(u) = \begin{pmatrix} D_p & & & \\ & R_1 & & \\ & & \ddots & \\ & & & R_r \end{pmatrix}$ avec D_p diagonale, $R_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ et $a_k \neq 0$ tels que $p + 2r = n$.

III] Rang d'applications

1] Point de vue endomorphisme

Proposition 23 : Soit $f : E \to E'$ application linéaire et F sous-espace vectoriel de E.
Alors : $f(F)$ est un sous-espace vectoriel de E'. En particulier $f(E)$ est appelé image de f, noté $\mathrm{Im}(f)$ et sa dimension est appelé rang de f : $\mathrm{rg}(f) := \dim(\mathrm{Im}(f))$.

Exemple 24 : Soit $E = E_1 \oplus E_2$ et p_{E_1} le projecteur sur E_1 parallèlement à E_2. $\mathrm{Im}(p_{E_1}) = E_1$ et $\ker(p_{E_1}) = E_2$

Théorème 25 : Deux espaces vectoriels de dimension finie sont isomorphes ssi ils ont même dimension.

Théorème 26 : (du rang) Soit $f : E \to E'$ application linéaire.
Alors : $\dim(E) = \mathrm{rg}(f) + \dim(\ker(f))$

Corollaire 27 : Soit $f \in \mathcal{L}(E; E')$ avec $\dim(E) = \dim(E')$.
Alors : f est injective ssi f est surjective ssi f est bijective

Contre-exemple 28 : Ceci est faux en dimension infinie.
Soit $D : \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P' \end{array}$. D est surjective, non-injective.

2] Point de vue matriciel

Définition 29 : Le rang de $A = (C_1 | \dots | C_n) \in \mathcal{M}_{p,n}(\mathbb{K})$ est la dimension de l'espace engendré par les vecteurs $C_1, \dots, C_n$, on le note :
$\mathrm{rg}(A) := \dim(\mathrm{Vect}(C_1, \dots, C_n))$

Proposition 30 : Soit $f \in \mathcal{L}(E; E')$ et $A = \mathrm{Mat}_{\mathcal{B}}(f)$
Alors : $\mathrm{rg}(f) = \mathrm{rg}(A)$

Définition 31 : Une matrice extraite de $A = (a_{i,j}) \in \mathcal{M}_{m,n}(\mathbb{K})$ est $A_{I,J} = (a_{i,j})$ avec $I = \{1 \leq i_1 < \dots < i_q \leq m\}$ et $J = \{1 \leq j_1 < \dots < j_p \leq n\}$
Un déterminant extrait de A est le déterminant d'une matrice carrée extraite.

Théorème 32 : Le rang d'une matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est l'ordre du plus grand déterminant extrait de A qui est non-nul.

Remarque 33 : En pratique, on utilise l'algorithme de Gauss pour déterminer le rang d'une matrice.

3] Point de vue bilinéaire et quadratique

Soit par la suite $\varphi \in \mathcal{L}_2(E)$ forme bilinéaire sur E et $q \in \mathcal{Q}(E)$ forme quadratique sur E et on suppose $\mathrm{car}(\mathbb{K}) \neq 2$.

Définition 34 : Soit $\mathcal{B} = (e_i)_{i=1}^n$ base de E. La matrice de φ dans la base $\mathcal{B}$ est : $\mathrm{Mat}_{\mathcal{B}}(\varphi) = (\varphi(e_i; e_j))_{1 \leq i,j \leq n}$.

Proposition 35 : Le rang de $\mathrm{Mat}_{\mathcal{B}}(\varphi)$ ne dépend pas de $\mathcal{B}$.

Définition 36 : Le rang de φ est le rang de $\mathrm{Mat}_{\mathcal{B}}(\varphi)$ dans n'importe quelle base $\mathcal{B}$.
On dit que φ est non-dégénérée si $\mathrm{rg}(\varphi) = \dim(E)$.

Proposition 37 : φ est non-dégénérée ssi pour toute base $\mathcal{B}$ de E, $\det(\mathrm{Mat}_{\mathcal{B}}(\varphi)) \neq 0$

Définition 38 : Le noyau de φ est $\ker(\varphi) = \{y \in E \mid \forall x \in E, \varphi(x; y) = 0\}$

Proposition 39 : $\dim(E) = \mathrm{rg}(\varphi) + \dim(\ker(\varphi))$

Définition 40 : Le noyau, rang et matrice de q sont ceux de φ sa forme polaire associée.

Remarque 40 : Le noyau de q n'est pas égal à $C_q = \{x \in E \mid q(x) = 0\}$ il s'agit du cône isotrope et vérifie $\ker(\varphi) \subseteq C_q$.

Exemple 41 : Soit $q(x) = x_1^2 + x_2^2 - x_3^2$. On a alors :
$\mathrm{rg}(q) = 3$ et $C_q = \{(x_1; x_2; x_3) \mid x_3 = \pm\sqrt{x_1^2 + x_2^2}\}$

III.2 [Gri°] [Gri°] III.8 [Gri°] XVII.4 [Rem] XVII.4 [Rem] IX.2 [Gri°] IX.4

III] Notion de dimension pour les extensions de corps

1] Extension finie de corps

Définition 42 : Une extension du corps $\mathbb{K}$ est la donnée de $(\mathbb{L}; \sigma)$ avec $\mathbb{L}$ un corps et $\sigma : \mathbb{K} \to \mathbb{L}$ morphisme de corps.
On note $\mathbb{L}/\mathbb{K}$.

Remarques 43 : (1) Le morphisme $\sigma : \mathbb{K} \to \mathbb{L}$ est injectif, on peut alors identifier $\mathbb{K}$ à un sous-corps de $\mathbb{L}$.
(2) Le corps $\mathbb{L}$ peut être muni d'une structure de $\mathbb{K}$-algèbre
Sa dimension étant appelé degré de l'extension noté : $[\mathbb{L} : \mathbb{K}]$
en tant que $\mathbb{K}$-espace vectoriel.

Définition 44 : Pour $\omega \in \mathbb{L}$, on note $\mathbb{K}[\omega] = \{P(\omega) \mid P \in \mathbb{K}[X]\}$
et $\mathbb{K}(\omega)$ le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et ω.
On dit que ω est algébrique sur $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X] \setminus \{0\}$
tel que $P(\omega) = 0$.
On dit que $\mathbb{L}$ est un corps de rupture de $P \in \mathbb{K}[X] \setminus \{0\}$ s'il existe
$\omega \in \mathbb{L}$ racine de P tel que $\mathbb{L} = \mathbb{K}[\omega]$.

Théorème 45 : Soit $P \in \mathbb{K}[X]$ irréductible de degré $n \geq 1$.
Alors : $\frac{\mathbb{K}[X]}{\langle P \rangle}$ est un corps de rupture de P et P est le polynôme
minimal de $\omega = \overline{X}$ sur $\mathbb{K}$.

Corollaire 46 : Pour tout $Q \in \mathbb{K}[X]$ de degré $n \geq 1$, il existe un
corps de rupture $\mathbb{L}$ de Q tel que $[\mathbb{L} : \mathbb{K}] \leq n$

2] Factorisation de polynômes sur un corps fini

Proposition 47 : L'application $S : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q \end{array}$ est un
$\mathbb{F}_q$-endomorphisme de l'espace vectoriel $\mathbb{F}_q[X]$.

Lemme 48 : Soit $\mathbb{L}/\mathbb{F}_q$ et $x \in \mathbb{L}$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$

Théorème 49 : (des restes chinois) Soit $(P_1; \dots; P_r) \in \mathbb{F}_q[X]$
polynômes premiers entre eux et $P = \prod_{i=1}^{r} P_i$
Alors : l'application $\frac{\mathbb{F}_q[X]}{\langle P \rangle} \to \frac{\mathbb{F}_q[X]}{\langle P_1 \rangle} \times \dots \times \frac{\mathbb{F}_q[X]}{\langle P_r \rangle}$
$$Q \bmod(P) \mapsto \left(Q \bmod(P_1); \dots; Q \bmod(P_r)\right)$$
est un isomorphisme de $\mathbb{F}_q$-algèbres

Théorème 50 : Soit $q = p^n$ avec p premier, $P \in \mathbb{F}_q[X]$ sans
facteurs carrés et $P = \prod_{i=1}^{r} P_i$ la décomposition de P en
produit d'irréductibles sur $\mathbb{F}_q[X]$.
Alors : (1) Si $r = 1$, alors P est irréductible
(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que
$PGCD(P; V - a)$ est facteur non-trivial de P.

Références :

[Gri] Algèbre Linéaire - Grifone

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[Isen] L'oral à l'agrégation de mathématiques - Isenmann