Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Mohamed NASSIRI

La notion de *sous-espace stable* est fondamentale pour les endomorphismes. Elle permet, par exemple, pour un s.e.v. F de E et $f \in \mathcal{L}(E)$, de considérer la restriction $f_{|F}$ qui est encore un endomorphisme de F. Cette propriété est essentielle notamment pour les raisonnements par récurrence.

Les sous-espaces stables sont très présents pour la réduction des endormorphismes. Le point de départ de notre affaire est la décomposition d'un espace E en somme de sous-espaces stables E_i sur lesquels un endomorphisme considéré u est "plus simple". En particulier, si les $u_{|E_i}$ sont des homothéties, u est *diagonalisable*. L'avantage de la dimension finie est la description matricielle d'un endomorphisme (via le choix d'une base). Diagonaliser un endomorphsime, c'est donc diagonaliser sa matrice.

La condition d'être une homothétie peut paraître très restrictive, voire utopique mais la densité des matrices diagonalisables $\mathcal{D}_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$ et la décomposition de Dunford de n'importe quelle matrice M de $\mathcal{M}_n(\mathbb{C})$ sous la forme $M = D + N$ avec $D \in \mathcal{M}_n(\mathbb{C})$ diagonalisable et $N \in \mathcal{M}_n(\mathbb{C})$ nilpotente (vérifiant en outre $DN = ND$), nous montre que l'étude des endomorphismes diagonalisables n'est pas superflue.

Deux outils vont être importants : le polynôme caractéristique et le polynôme minimal. Des conditions simples sur ces polynômes vont nous donner des critères de diagonalisation, et le célèbre théorème de Cayley-Hamilton nous donne une relation de divisibilité entre ces deux polynômes.

Par la suite, on se place dans un espace euclidien et donc on aura plein de propriétés géométriques, notamment grâce au produit scalaire. A partir de la définition des endomorphismes adjoints, c'est-à-dire que l'on se donne un endomorphisme $f \in \mathcal{L}(E)$, et on a l'existence d'un et d'un seul endomorphisme f^* de E tel que

$$\langle f(x), y\rangle = \langle x, f^*(y)\rangle \quad \forall x, y \in E$$

On va s'intéresser aux relations suivantes entre f et f^* :

$$\begin{tikzcd}
 & \boxed{Endomorphismes\ f\ et\ f^*} \arrow[dl] \arrow[d] \arrow[dr] & \\
\boxed{f^* = f} \arrow[d] & \boxed{f^* \circ f = f \circ f^*} \arrow[d] & \boxed{f^* \circ f = f \circ f^* = Id} \arrow[d] \\
\boxed{autoadjoints} & \boxed{normaux} & \boxed{orthogonaux}
\end{tikzcd}$$

On sait que $\mathbb{C}$ est algébriquement clos d'après le théorème de D'Alembert-Gauss, donc il est inutile de vouloir chercher un sur-corps de $\mathbb{C}$. Cepedant, si l'on sacrifie la commutativité, on peut créer un sur-corps de $\mathbb{C}$: le corps des quaternions $\mathbb{H}$. Le lien entre quaternions et transformations géométriques est donné par l'isomorphisme :

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

où G est le groupe des quartenions de norme 1. Ce qui permet de faire explicitement le lien entre les quaternions et les rotations dans l'espace sont les *formules de rotation d'Olinde Rodrigues.*

Pour finir, en considèrant un $\mathbb{C}$-espace vectoriel V de dimension finie n, on introduira la notion de *représentation linéaire*. Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme $\rho : G \to \mathrm{GL}(V)$. Par la suite, on s'intéresse à la *décomposition* des représentations dites *irréductibles* dans le sens suivant : si une représentation ρ de G sur V admet un sous-espace vectoriel $W \subset V$ stable pour tous les $\rho(g) \in \mathrm{GL}(V)$, elle induit une représentation ρ_W sur W appelée *sous-représentation.* Par la suite, une représentation sur un espace V est dite irréductible si elle admet exactement deux sous-représentations : $\{0\}$ et V tout entier. Les deux résultats qui méritent d'être mis en avant sont le *théorème de Maschke* et le *lemme de Schur.*

Références

[GRI] Algèbre linéaire 5e Edition, Joseph Grifone
[OBJ] Objectif Agrégation, Vincent Beck, Jérôme Malick et Gabriel Peyré
[PEY] L'algèbre discrète de la transformée de Fourier, Gabriel Peyré
[MADal] Leçons d'Algèbre : Préparation à l'Oral de l'Agrégation, Karine Madère
[GOUal] Les maths en tête : Algèbre, Xavier Gourdon ♠
[PER] Cours d'Algèbre, Daniel Perrin ♠

Développements

Théorème des polynômes annulateurs et Décomposition de Dunford
$SO_3(\mathbb{R})$ et les quaternions

Dans cette leçon, K est un corps commutatif et E un K-e.v. de dimension finie.

1 Définitions et premières propriétés [MADal] p.220-221

1.1 Sous-espaces stables

Définition 1 *Soit F un s.e.v. de E et $f \in \mathcal{L}(E)$. On dit que F est stable par f si l'on a $f(F) \subset F$.*

Exemple 2 *Soit $f \in \mathcal{L}(E)$ et $P \in K[X]$. Alors $\mathrm{Im}P(f)$ et $\mathrm{Ker}P(f)$ sont deux sous-espaces vectoriels de E stables par f.*

Proposition 3 *Lemme des noyaux*
Soit $f \in \mathcal{L}(E)$ et $Q(X) = Q_1(X)...Q_p(X)$ un polynôme factorisé en produit de polynômes deux à deux premiers entre eux.
Si $Q(f) = 0$, alors

$$E = \mathrm{Ker}Q_1(f) \oplus ... \oplus \mathrm{Ker}Q_p(f)$$

[GRI] p.179-180

Exemple 4 *Soit $f \in \mathcal{L}(E)$. On appelle espace propre de f tout sous-espace vectoriel de E égal à $\mathrm{Ker}(f - \lambda \mathrm{Id}_E)$ où λ est une valeur propre de f.*
Alors espace propre de f est stable par f.

Exemple 5 *Soit $f \in \mathcal{L}(E)$ tel que son polynôme caractéristique $\chi_f(X) = (-1)^n(X-\lambda_1)^{\alpha_1}...(X-\lambda_p)^{\alpha_p}$ soit scindé. On appelle espace caractéristique associé à la valeur propre λ_i le sous-espace vectoriel*

$$N_{\lambda_i} = \mathrm{Ker}(f - \lambda_i \mathrm{id})^{\alpha_i}$$

Alors espace caractéristique de f est stable par f.

1.2 Endomorphismes induits et propriétés

Proposition 6 *Soit $f \in \mathcal{L}(E)$ et F un s.e.v. de E stable par f. Alors l'application*

$$\begin{aligned} f_{|F} : F &\to F \\ x &\mapsto f(x) \end{aligned}$$

est un endomorphisme de F.

Proposition 7 *Soit $f \in \mathcal{L}(E)$ et F un sous-espace vectoriel de E stable par f.*
De plus, on note χ_f, π_f, $\chi_{f_{|F}}$ et $\pi_{f_{|F}}$ respectivement le polynôme caractéristique de f, le polynôme minimal de f, le polynôme caractéristique de $f_{|F}$, et le polynôme minimal de $f_{|F}$.
Alors $\chi_{f_{|F}}$ divise χ_f et si $F \neq \{0\}$, $\pi_{f_{|F}}$ divise π_f.

Proposition 8 *Soient $f, g \in \mathcal{L}(E)$ tels que $f \circ g = g \circ f$. Alors*
(i) Tout sous-espace propre de f est stable par g (en particulier $\mathrm{Ker}f$).
(ii) $\mathrm{Im}f$ est stable par g.

Définition 9 *Soient E et F deux espaces vectoriels de dimension quelconque. Soit $u \in \mathcal{L}(E, F)$. On définit l'application transposée de u, notée ${}^t u$, comme suit*

$$\begin{aligned} {}^t u : F^* &\to E^* \\ f &\mapsto f \circ u \end{aligned}$$

Proposition 10 *Supposons E de dimension finie. Soit $f \in \mathcal{L}(E)$. Un s.e.v. F de E est stable par f si et seulement si $F^{\perp}$ est stable par ${}^t f$.*

2 Réduction des endomorphismes

2.1 Diagonalisation [GRI] p.153 → 183

Définition 11 *On dira que $f \in \mathcal{L}(E)$ est diagonalisable s'il existe une base (e_i) telle que*

$$M(f)_{e_i} = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}$$

Théorème 12 (I) *$f \in \mathcal{L}(E)$ est diagonalisable si et seulement s'il existe une base de E formée de vecteurs propres.*

Théorème 13 (II) *Soient $f \in \mathcal{L}(E)$ et $\lambda_1, ..., \lambda_p$ les valeurs propres de f. Alors les propositions suivantes sont équivalentes :*
(i) f est diagonalisable.
(ii) $E = E_{\lambda_1} \oplus ... \oplus E_{\lambda_p}$.
(iii) $\dim E = \dim E_{\lambda_1} + ... + \dim E_{\lambda_p}$

Corollaire 14 *Si f admet n valeurs propres deux à deux distinctes, alors f est diagonalisable.*

Proposition 15 *Soient $f \in \mathcal{L}(E)$ et λ une valeur propre d'ordre α de f. Alors* $\dim E_\lambda \leq \alpha$

Théorème 16 (III) *Soit $f \in \mathcal{L}(E)$. Alors f est diagonalisable si et seulement si :*
(i) $\chi_f(X)$ est scindé dans K (i.e.)

$$\chi_f(X) = (-1)^n (X - \lambda_1)^{\alpha_1} ... (X - \lambda_p)^{\alpha_p}$$

avec $\lambda_1, ..., \lambda_p \in K$, et $\alpha_1 + ... + \alpha_p = n$
(ii) Les dimensions des espaces propres sont maximales (i.e.) $\forall i \in \{1, ..., n\}$, $\dim E_{\lambda_i} \leq \alpha_i$

Exemple 17 • $A = \begin{pmatrix} 2 & 0 & 4 \\ 3 & -4 & 12 \\ 1 & -2 & 5 \end{pmatrix}$ *est diagonalisable.*
• $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ *est diagonalisable.*
• $A = \begin{pmatrix} -4 & 0 & -2 \\ 0 & 1 & 0 \\ 5 & 1 & 3 \end{pmatrix}$ *n'est pas diagonalisable.*

Proposition 18 *Soient $f \in \mathcal{L}(E)$ et $\chi_f(X) = (-1)^n (X - \lambda_1)^{\alpha_1} ... (X - \lambda_p)^{\alpha_p}$ son polynôme caractéristique. Alors, si f est diagonalisable, $Q(X) = (X - \lambda_1)...(X - \lambda_p)$ annule f.*

Théorème 19 (IV) *$f \in \mathcal{L}(E)$ est diagonalisable si et seulement s'il existe un polynôme annulateur de f, scindé et n'ayant que des racines simples.*

Théorème 20 (V) *$f \in \mathcal{L}(E)$ est diagonalisable si et seulement si son polynôme minimal est scindé et à racines simples.*

Exemple 21 • $A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ *est diagonalisable.*
• $A = \begin{pmatrix} 3 & 2 & -2 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ *n'est pas diagonalisable.*

2.2 Trigonalisation [GRI] p.153 → 174

Définition 22 *On dira que $f \in \mathcal{L}(E)$ est trigonalisable s'il existe une base (e_i) telle que*

$$M(f)_{e_i} = \begin{pmatrix} a_{11} & * & \dots & * \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}$$

Théorème 23 *$f \in \mathcal{L}(E)$ est trigonalisable si et seulement si son polynôme caractéristique est scindé (i.e.)*

$$\chi_f(X) = (-1)^n (X - \lambda_1)^{\alpha_1} ... (X - \lambda_p)^{\alpha_p}$$

avec $\lambda_1, ..., \lambda_p \in K$, et $\alpha_1 + ... + \alpha_p = n$

Corollaire 24 *Tout matrice $A \in \mathcal{M}_n(\mathbb{C})$ est semblable à une matrice triangulaire de $\mathcal{M}_n(\mathbb{C})$.*

Exemple 25 $A = \begin{pmatrix} -4 & 0 & -2 \\ 0 & 1 & 0 \\ 5 & 1 & 3 \end{pmatrix}$ *est semblable à* $A' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$

Corollaire 26 *Soit $A \in \mathcal{M}_n(K)$ et* $\mathrm{Sp}A = \{\lambda_1, ..., \lambda_p\}$. *On a alors*

$$\mathrm{Tr}A = \lambda_1 + ... + \lambda_p$$
$$\det A = \lambda_1 \times ... \times \lambda_p$$

2.3 Réductions simultanées [GOUal] p.166 → 173

Théorème 27 *<u>Réductions simultanées</u>*
Soient $f, g \in \mathcal{L}(E)$ diagonalisables (resp. trigonalisables) et tels que $f \circ g = g \circ f$. Alors il existe une base commune de diagonalisation (resp. trigonalisation) de f et g.
On dit alors que f et g sont <u>codiagonalisables</u> (resp. <u>cotrigonalisables</u>).

Corollaire 28 *Soit $(f_i)_{i \in I}$ une famille d'endomorphismes de E diagonalisables (resp. trigonalisables) et commutant deux à deux. Alors il existe une base commune de diagonalisation (resp. trigonalisation) à tous les f_i.*

Application 29 *Lemme de Schur*
Soit E un $\mathbb{C}$-e.v. de dimension finie. Soit $Q \subset End_{\mathbb{C}}(E)$ irréductible (c'est-à-dire que les seuls sous-espaces de E stables par tous les éléments de Q sont $\{0\}$ et E). Alors les seuls éléments commutant avec tous les éléments de Q sont les homothéties.

Remarque 30 *Si E est un $\mathbb{R}$-e.v. de dimension finie, le résultat est faux !*
Cependant, si $\dim E$ est impair, le résultat reste vrai.

2.4 Décomposition de Dunford [GOUal] p.192-193

Théorème 31 ♠ *Théorème des polynômes annulateurs* ♠
Soit $f \in L(E)$ et $F \in \mathbb{K}[X]$ tel que $F(f) = 0$. Soit $F = \beta M_1^{\alpha_1}...M_s^{\alpha_s}$ la décomposition de Dunford en facteurs irréductibles de $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = KerM_i^{\alpha_i}(f)$. On a alors $E = N_1 \bigoplus ... \bigoplus N_s$ et pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$ est un polynôme en f.

Théorème 32 ♠ *Décomposition de Dunford* ♠
Soit $f \in L(E)$ tel que son polynôme caractéristique χ_f soit scindé sur $\mathbb{K}$. Alors, il existe un unique couple (d, n) d'endomorphismes tel que :
(i) d est diagonalisable, n est nilpotente.
(ii) $f = n + d$ et $d \circ n = n \circ d$.
De plus, d et n sont des polynômes en f.

Proposition 33 *Soient $A \in \mathcal{M}_n(\mathbb{C})$ tel que son polynôme minimal π_A soit scindé et $A = D + N$ la décomposition de Duford dans $\mathbb{C}$ de A. On considère l'application*

$$\begin{aligned}\varphi_A := [A, .] : \ & \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})\\ & M \mapsto AM - MA\end{aligned}$$

(i) Alors $\varphi_A = \varphi_D + \varphi_N$ est la décomposition de Duford de φ_A.
(ii) (A est diagonalisable) $\Leftrightarrow$ (φ_A est diagonalisable).

3 Endomorphismes remarquables

3.1 Endomorphismes cycliques [OBJ] p.174 → 175

Définition-Proposition 34 *A un polynôme unitaire*

$$P(X) = X^n - a_{n-1}X^{n-1} - ... - a_0 \in K[X]$$

on associe sa matrice compagnon définie par

$$C_P = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & a_0 \\ 1 & 0 & \dots & \dots & 0 & a_1 \\ 0 & 1 & \ddots & \vdots & 0 & \vdots \\ 0 & 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 0 & 1 & a_{n-1} \end{pmatrix} \in \mathcal{M}_n(K)$$

On a $\chi_{C_P} = P$.

Définition 35 *Soient E un k-e.v. de dimension n et $u \in \mathbb{L}(E)$. On dit que u est cyclique s'il existe $x \in E$ tel que*

$$(x, u(x), ..., u^{n-1}(x))$$

soit une base de E.

Proposition 36 *Soient E un K-e.v. de dimension n eu $u \in \mathcal{L}(E)$. Les propositions suivantes sont équivalentes :*
(i) u est cyclique ;
(ii) $(-1)^n\chi_u = \pi_u$;
(iii) π_u est de degré n ;
(iv) il existe une base de E dans laquelle la matrice de E est une matrice compagnon ;
(v) $\dim(K[u]) = n$.

Proposition 37 *Soient E un K-e.v. de dimension n eu $u \in \mathcal{L}(E)$. Alors u est diagonalisable si et seulement s'il admet n valeurs propres distinctes.*

3.2 Endomorphismes autoadjoints et normaux [GRI] p.252 → 254, p.286-287

Définition 38 *Un endomorphisme f d'un espace euclidien est dit autoadjoint si*

$$\langle f(x), y\rangle = \langle x, f(y)\rangle \quad \forall x, y \in E$$

En d'autres termes, f est autoadjoint si $f^* = f$.
Matriciellement, f est autoadjoint si et seulement si la matrice qui le représente dans une base orthonormée est symétrique.

Proposition 39 *Soit E un espace euclidien et $f \in \mathcal{L}(E)$ un endomorphisme autoadjoint. Si F est un s.e.v. de E stable par f, alors $F^\perp$ est stable par f.* **[GOUal] p.244**

Théorème 40 *Soit f un endomorphisme autoadjoint d'un espace euclidien. Alors :*
(i) f est diagonalisable.
(ii) Les sous-espaces propres de f sont deux à deux orthogonaux.

Corollaire 41 *Soit $A \in \mathcal{S}_n(\mathbb{R})$. Il existe alors $P \in O_n(\mathbb{R})$ telle que la matrice $A' =^t PAP$ soit diagonale.*

Remarque 42 *Les matrices symétriques complexes (non réelles) ne sont pas nécessairement diagonalisables (ni dans* $\mathbb{R}$*, ni dans* $\mathbb{C}$*). Par exemple,* $A = \begin{pmatrix} 0 & 1 \\ 1 & 2i \end{pmatrix}$ *est symétrique et non diagonalisable.*

Définition 43 *Un endomorphisme f d'un espace hermitien est dit* <u>*normal*</u> *si*

$$f^* \circ f = f \circ f^*$$

Matriciellement, f est normal si et seulement si la matrice $A \in \mathcal{M}_n(\mathbb{C})$ *qui le représente dans une base orthonormée est normale* (${}^t\overline{A}A = A^t\overline{A}$)*.*

Exemple 44 *En particulier sont normales, les matrices (anti)symétriques réelles, hermitiennes, orthogonales et unitaires.*

Proposition 45 *Soit E un espace hermitien et* $f \in \mathcal{L}(E)$ *un endomorphisme autoadjoint. Si F est un s.e.v. de E stable par f, alors* $F^\perp$ *est stable par* f^**.* **[GOUal] p.258**

Théorème 46 *Soit f un endomorphisme normal d'un espace hermitien. Alors :*
(i) f est diagonalisable.
(ii) Les sous-espaces propres de f sont deux à deux orthogonaux.

Corollaire 47 *Soit* $A \in \mathcal{M}_n(\mathbb{C})$ *normale. Il existe alors* $U \in U_n$ *telle que la matrice* $A' = {}^t\overline{U}AU$ *soit diagonale (non nécessairement réelle).*

3.3 Endormorphismes orthogonaux [GRI] p.239 → 241

Définition 48 $f \in \mathcal{L}(E)$ *est dit* <u>*endormorphisme orthogonal*</u> *si*

$$\langle f(x), f(y)\rangle = \langle x, y\rangle \quad \forall x, y \in E$$

On note $O(E)$ *l'ensembles des endomorphismes orthogonaux de E.*

Proposition 49 *Soit* $f \in \mathcal{L}(E)$*. Les propositions suivantes sont équivalentes :*
(i) $\langle f(x), f(y)\rangle = \langle x, y\rangle \quad \forall x, y \in E$
(ii) $||f(x)|| = ||x|| \quad \forall x \in E$
(iii) Si $\mathcal{B} = (e_1, ..., e_n)$ *une base orthonormée de E et* $A = Mat(f)_\mathcal{B}$*, alors* ${}^tAA = A^tA = I_n$

Proposition-Définition 50 *Soit* $f \in O(E)$*, alors :*
(i) Les valeurs propres de f sont +1 et -1.
(ii) $\det f = \pm 1$*. En particulier, f est bijective.*
Les endomorphismes orthogonaux de déterminant +1 sont dites <u>*directes*</u> *; celles de déterminant -1 sont dites* <u>*indirectes*</u>*.*

Proposition 51 *f est un endomorphisme orthogonal si et seulement si elle transforme toute base orthonormée en une base orthonormée.*
Pour cela, il suffit qu'il existe une base orthonormée qui, par f, est transformée en une base orthonormée.

Proposition 52 *Soit E un espace euclidien ou hermitien et* $f \in \mathcal{L}(E)$ *un endomorphisme orthogonal. Si F est un s.e.v. de E stable par f, alors* $F^\perp$ *est stable par f.* **[GOUal] p.244**

Théorème 53 *Soient E un espace euclidien et* $f \in \mathcal{L}(E)$ *un endomorphisme orthogonal. Alors il existe une base orthonormale* $\mathcal{B}$ *de E telle que*

$$Mat(f)_\mathcal{B} = \begin{pmatrix} R(\theta_1) & & & & & \\ & \ddots & & & 0 & \\ & & R(\theta_r) & & & \\ & & & \epsilon_1 & & \\ & 0 & & & \ddots & \\ & & & & & \epsilon_s \end{pmatrix},$$

où pour tout j, $\epsilon_j \in \{\pm 1\}$ *et pour tout i,*

$$R(\theta_i) = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$$

avec $\theta_i \in \mathbb{R},\ \theta_i \not\equiv 0 \pmod{\pi}$ **[GOUal] p.256-257**

4 Quaternions [PER] p.160 → 164

Proposition-Définition 54 *Il existe une algèbre* $\mathbb{H}$ *de dimension 4 sur* $\mathbb{R}$*, appelé* <u>*algèbre des quaternions*</u>*, muni d'une base 1,i,j,k telle que :*
(i) 1 est élément neutre pour la multiplication,
(ii) on a les formules

$$jk = -kj = i, \quad ki = -ik = j, \quad ij = -ji = k$$

$$i^2 = j^2 = k^2 = -1$$

Un quaternions s'écrit alors

$$q = a + bi + cj + dk, \quad \text{avec } a, b, c, d \in \mathbb{R}$$

Définition 55 $\mathbb{H}$ *est muni de la* <u>*norme algébrique*</u> *N suivante :* $\forall\ q = a + bi + cj + dk \in \mathbb{H}$

$$N(q) = a^2 + b^2 + c^2 + d^2$$

Théorème 56 ♠ <u>$SO_3(\mathbb{R})$ *et les quaternions*</u> ♠ *Soit G le groupe des quaternions de norme 1. On a l'isomorphisme suivant :*

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

5 Représentations linéaires de groupes

5.1 Définitions et premières propriétés [PEY] p.194-195

Définition 57 *Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme $\rho : G \to \mathrm{GL}(V)$. Ceci correspond à la donnée d'une action linéaire du groupe G sur V :*

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto g.v = \rho(g)(v) \end{aligned}$$

Une représentation ρ est dite fidèle si ρ est injective. On dit aussi que G agit fidèlement sur V.

Définition 58 *On définit $\mathbb{C}[G]$ l'espace vectoriel de dimension $|G|$ sur $\mathbb{C}$ dont la base est indexée par G et de la forme $\{e_g\}_{g\in G}$.*

Remarque 59 *Pour $g \in G$, on note*

$$\delta_g : \begin{cases} G & \to \mathbb{C} \\ h & \mapsto \begin{cases} 1 & si\ h = g \\ 0 & sinon \end{cases} \end{cases}$$

Par suite, pour une fonction $f : G \to \mathbb{C}$, on a

$$f = \sum_{g\in G} f(g)\delta_g$$

Ce qui permet d'identifier $\mathbb{C}[G]$ avec l'espace des fonctions de G sans $\mathbb{C}$.

5.2 Exemples fondamentaux [PEY] p.195 → 198

Exemple 60 *La représentation régulière à gauche est la représentation de G sur l'espace vectoriel $\mathbb{C}[G]$ (espace vectoriel de dimension $|G|$ sur $\mathbb{C}$ dont la base est indexée par G et de la forme $\{e_g\}_{g\in G}$) définie par le morphisme*

$$\forall g \in G, \quad \rho(g) : \begin{cases} \mathbb{C}[G] & \to \mathbb{C}[G] \\ e_h & \mapsto e_{gh} \end{cases}$$

Proposition 61 *La représentation régulière est fidèle.*

Définition 62 *Pour deux représentations ρ_V et ρ_W respectivement sur V et W, on définit une représentation somme $\rho_{V\oplus W}$ par*
$\forall g \in G,\ \forall (v, w) \in V \times W,$

$$\rho_{V\oplus W}(g)((v, w)) := \rho_V(g)(v) + \rho_W(g)(w)$$

Définition 63 *Pour deux représentations ρ_V et ρ_W respectivement sur V et W, on définit une représentation des morphimes $\rho_{\mathcal{L}(V,W)}$ sur $\mathcal{L}(V, W)$ par*
$\forall g \in G,\ \forall f \in \mathcal{L}(V, W),$

$$\rho_{\mathcal{L}(V,W)}(g)(f) := \rho_W(g) \circ f \circ \rho_V(g^{-1})$$

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_V(g)"'] & W \arrow[d, "\rho_W(g)"] \\ V \arrow[r, "\rho_{\mathcal{L}(V,W)}(g)"'] & W \end{tikzcd}$$

Proposition 64 *On définit bien ainsi une proposition.*

Définition 65 *On définit l'action de $\mathfrak{S}_n$ sur $\mathbb{C}[X_1, ..., X_n]$ par*

$$\begin{aligned} \mathfrak{S}_n \times \mathbb{C}[X_1, ..., X_n] &\to \mathbb{C}[X_1, ..., X_n] \\ (\sigma, P(X_1, ..., X_n)) &\mapsto \sigma.P(X_1, ..., X_n) \\ &= P(X_{\sigma(1)}, ..., X_{\sigma(n)}) \end{aligned}$$

[GOUal] p.78

5.3 Représentations irréductibles [PEY] p.198 → 201

Définition 66 • *Soient ρ et ρ' deux représentations d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V'. Un opérateur d'entrelacement est une application linéaire $\tau : V \to V'$ tel que pour tout $g \in G$, $\tau \circ \rho(g) = \rho'(g) \circ \tau$*

$$\begin{tikzcd} V \arrow[r, "\tau"] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\ V \arrow[r, "\tau"] & V' \end{tikzcd}$$

• *On note $\mathrm{Hom}_G(V, V')$ l'ensemble des opérateurs d'entrelacements.*
• *Deux représentations ρ et ρ' d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' sont dites isomorphes (ou G-isomorphes) si τ est bijective.*

Définition 67 *Si une représentation ρ de G sur V admet un sous-espace vectoriel $W \subset V$ stable pour tous les $\rho(g) \in \mathrm{GL}(V)$, elle induit une représentation ρ_W sur W appelée sous-représentation.*

Définition 68 *Une représentation sur un espace V est dite irréductible si elle admet exactement deux sous-représentations : $\{0\}$ et V tout entier.*

Définition-Proposition 69 *Soit ρ une représentation de G sur V. Alors ρ laisse invariant le produit hermitien suivant :*

$$\langle x, y\rangle_G := \sum_{g\in G} \langle \rho(g)(x), \rho(g)(y)\rangle$$

où $\langle .,. \rangle$ est un produit hermitien quelconque sur V. On dit alors que ρ est une représentation unitaire.

Théorème 70 *Théorème de Maschke*
Toute représentation peut s'écrire comme somme de représentations irréductibles.

5.4 Invariance et représentations [PEY] p.203 → 205

Définition 71 *Soit ρ une représentation sur V. On note*

$$V^G = \{v \in V \mid \forall g \in G,\ \rho(g)(v) = g.v = v\}$$

C'est une sous-représentation de V.

Exemple 72 *En considérant l'action de $\mathfrak{S}_n$ sur $\mathbb{C}[X_1, ..., X_n]$, on dit qu'un polynôme $P \in \mathbb{C}[X_1, ..., X_n]$ est symétrique si $P \in \mathbb{C}[X_1, ..., X_n]^{\mathfrak{S}_n}$ (i.e.) si $\forall \sigma \in \mathfrak{S}_n$, on a*

$$P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$$

[GOUal] p.78

Exemple 73 *Dans le cas de la représentation des morphimes $\rho_{\mathcal{L}(V,W)}$ sur $\mathcal{L}(V, W)$ de deux représentations ρ_V et ρ_W respectivement sur V et W, on a* $\mathrm{Hom}_G(V, V') = \mathcal{L}(V, W)^G$

Proposition 74 *Lemme de Schur :*
Soient ρ et ρ' deux représentations irréductibles d'un groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' et $f \in \mathcal{L}(V, V')$ un opérateur d'entrelacement. Alors
(i) si ρ et ρ' ne sont pas isomorphes, $f = 0$.
(ii) Si $f \neq 0$, alors f est un isomorphisme.
Si on suppose $V = V'$, alors f est une homothétie.

Corollaire 75 *On considère toujours deux représentations irréductibles d'un groupe G sur V et V'. On a donc*

$$\dim(\mathrm{Hom}_G(V, V')) = \begin{cases} 1 & \text{si } V \text{ et } V' \text{ sont isomorphes} \\ 0 & \text{sinon} \end{cases}$$

Questions

Exercice : Soient E un K-e.v. de dimension n eu $u \in \mathcal{L}(E)$.
1) Montrer que les propositions suivantes sont équivalentes :
(i) u est cyclique ;
(ii) $(-1)^n \chi_u = \pi_u$;
(iii) π_u est de degré n ;
(iv) il existe une base de E dans laquelle la matrice de E est une matrice compagnon ;
(v) $\dim(K[u]) = n$.
2) Montrer que u est diagonalisable si et seulement s'il admet n valeurs propres distinctes.

Solution : 1)
(i) ⇒ (iv) : Dans une base de la forme $(x, u(x), ..., u^{n-1}(x))$, la matrice de u est une matrice compagnon.

(iv) ⇒ (i) : Soit $\mathcal{B} = (e_1, ..., e_n)$ une base dans laquelle la matrice de u est une matrice compagnon. Alors, on a

$$\mathcal{B} = (e_1, u(e_1), ..., u^{n-1}(e_1))$$

(i) ⇒ (ii) : Comme u est cyclique, alors on a $\deg(\pi_u) \geq n = \deg \chi_u$. En effet, si on avait $\deg \pi_u \leq n-1$, alors la famille $(x, u(x), ..., u^{n-1}(x))$ serait liée. Par ailleurs, par le théorème de Cayley-Hamilton, $\pi_u \mid \chi_u$. Par conséquent, on en déduit que $(-1)^n \chi_u = \pi_u$.

(ii) ⇔ (iii) ⇔ (v) : Grâce à l'isomorphisme

$$K[u] \simeq K[X]/(\pi_u)$$

on a donc $\dim K[u] = \deg \pi_u$. Par ailleurs, toujours par le théorème de Cayley-Hamilton, $\pi_u \mid \chi_u$. Par conséquent, on en déduit que

$$(-1)^n \chi_u = \pi_u \Leftrightarrow \deg \pi_u = n \Leftrightarrow \dim(K[u]) = n$$

(iii) ⇔ (i) : C'est le point le plus délicat de la démonstration. Il demande quelques notions et résultats intermédiaires ...

• Polynôme minimal et noyau de polynôme d'endomorphisme :
On va montrer un résultat intéressant concernant les polynômes mininaux et les sous-espaces définis à partir d'un noyau de polynôme d'endomorphisme. Plus précisement, soient P et Q deux polynômes unitaires (non nécessairement premiers entre eux) tels que $\pi_u = PQ$ et notons $F = \mathrm{Ker} P(u)$. C'est un sous-espace stable par u.
Montrons que $\pi_F = \pi_{u_{|F}} = P$: Comme $P(u)(x) = 0$ pour tout $x \in F$, on a déjà $\pi_F \mid P$. De plus, pour $x \in E$, on a

$$P(u)(Q(u)(x)) = \pi_u(u)(x) = 0$$

et donc $Q(u)(x) \in F$. Par suite, $\pi_F \circ Q(u) = 0$, et on en déduit que $\pi_u \mid \pi_F Q$. Finalement, on a

$$\pi_u \mid \pi_F Q \mid PQ = \pi_u$$

Donc, on a égalité partout et ainsi $\pi_F = P$.

• **Une première définition de $\pi_{u,x}$:**
Soient $x \in E$ et F le sous-espace stable par u et engendré par x. Notons $\pi_{u,x}$ le polynôme minimal de la restriction de u à F. On a donc

$$\pi_{u,x} \mid \pi_u$$

• **Une deuxième définition de $\pi_{u,x}$:**
Par ailleurs, on a par définition de F,

$$F = \text{vect}(u^p(x)\ ;\ p \in \mathbb{N}) = \{P(u)(x)\ ;\ P \in K[X]\}$$

Comme pour démontrer l'existence du polynôme minimal, on va considérer l'application

$$\begin{aligned} \varphi_{u,x} : K[X] &\to F \\ P(X) &\mapsto P(u)(x) \end{aligned}$$

Son noyau $I = \{P \in K[X] \mid P(u)(x) = 0\}$ est un idéal de $K[X]$. Or l'idéal I n'est pas réduit à $\{0\}$ (deux arguments : soit parce que $\pi_u \in I$, soit parce que $\varphi_{u,x}$ ne peut pas être injectif entre un espace de dimension infinie et un espace de dimension finie). Notons donc Q le polynôme unitaire qui engendre cet idéal (tout idéal de $K[X]$ est engendré par un élément puisque que $K[X]$ est principal).

Montrons en fait que $Q = \pi_{u,x}$: Comme $\pi_{u,x}(u) = 0$ sur F, alors $\pi_{u,x}(u)(x) = 0$ et donc $\pi_{u,x} \in I$. Par suite, $Q \mid \pi_{u,x}$.
Réciproquement, montrons que $Q(u)(y) = 0$ pour tout $y \in F$ (ce qui nous donnera $\pi_{u,x} \mid Q$). Soit $y \in F$, il existe $P \in K[X]$ tel que $y = P(u)(x)$. Par suite,

$$Q(u)(y) = Q(u) \circ P(u)(x) = P(u) \circ Q(u)(x) = P(u)(0) = 0$$

Finalement Q annule $u_{|F}$, et donc $\pi_{u,x} \mid Q$. Par conséquent, on a $\pi_{u,x} = Q$.

• **Lien entre π_u et $\pi_{u,x}$:**
Montrons qu'il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$: On peut écrire

$$\pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$$

avec les P_i irréductibles et distincts deux à deux, d'où, par le lemme des noyaux, on a

$$E = \bigoplus_{i=1}^{r} \text{Ker}(P_i^{\alpha_i}(u))$$

Pour tout $y \in \text{Ker}(P_i^{\alpha_i}(u))$, $\pi_{u,y} \mid P_i^{\alpha_i}$ et donc $\pi_{u,y} = P_i^{\beta}$ avec $\beta \leq \alpha_i$ (car P_i est irréductible).
D'après notre premier point, $P_i^{\alpha_i}$ est le polynôme minimal de la restriction de u à $\text{Ker}(P_i^{\alpha_i}(u))$. Par suite, pour tout i, il existe $x_i \in \text{Ker}(P_i^{\alpha_i}(u))$ tel que $P_i^{\alpha_i - 1}(u)(x) \neq 0$ et on en déduit donc que $\pi_{u,x_i} \mid P_i^{\alpha_i}$.
Maintenant, posons $x = x_1 + ... + x_r$ et montrons que $\pi_{u,x} = \pi_u$. On a déjà $\pi_{u,x} \mid \pi_u$. Pour montrer que $\pi_u \mid \pi_{u,x}$, on va montrer que $P_i^{\alpha_i} \mid \pi_u$ pour tout i.
On a

$$0 = \pi_{u,x}(x) = \pi_{u,x}(x_1) + ... + \pi_{u,x}(x_r)$$

Pour tout i, $\text{Ker}(P_i^{\alpha_i}(u))$ est stable par u donc $\pi_{u,x}(x_i) \in \text{Ker}(P_i^{\alpha_i}(u))$. La somme étant directe, on en déduit que $\pi_{u,x}(x_i) = 0$ pour tout i (*i.e.*) $P_i^{\alpha_i} = \pi_{u,x_i} \mid \pi_{u,x}$. Comme les $P_i^{\alpha_i}$ sont premiers entre eux, on obtient

$$\prod_{i=1}^{r} P_i^{\alpha_i} = \pi_u \mid \pi_{u,x}$$

On peut (enfin !) revenir à notre démonstration ...
D'après nos remarques, il existe un élément $x \in E$ tel que $\pi_{u,x} = \pi_u$. Ainsi, $\text{deg}\pi_{u,x} = n$ et la famille $(x, u(x), ..., u^{n-1}(x))$ est libre. Par suite, comme la famille $(x, u(x), ..., u^{n-1}(x))$ est de cardinal n, c'est une base de E.

2) Notons λ_i, pour $1 \leq i \leq r$, les valeurs propres distinctes de u et E_i, pour $1 \leq i \leq r$, les espaces propres associés (avec *a priori* $r \leq n$).

<u>$\Rightarrow$:</u> Comme u est cyclique, il existe $x \in E$ tel que $(x, u(x), ..., u^{n-1}(x))$ soit une base de E. Comme u est diagonalisable, on a donc

$$E = \bigoplus_{i=1}^{r} E_i$$

Ainsi, on peut écrire $x = x_1 + ... + x_r$ avec $x_i \in E_i$, pour $1 \leq i \leq r$. Par ailleurs, le polynôme $P(X) = (X - \lambda_1)...(X - \lambda_r)$ vérifie $P(u)(x) = 0$. Mais comme la famille $(x, u(x), ..., u^{n-1}(x))$ est libre, on a $\deg P(X) = r \geq n$. En effet, dans le cas contraire, cela supposerait qu'il existe une relation de dépendance linéaire, et donc un polynôme $Q(X)$ de degré inférieur ou égal à $n-1$ tel que $Q(u)(x) = 0$, ce qui contredirait la liberté de la famille $(x, u(x), ..., u^{n-1}(x))$). Ainsi $r = n$, et donc u a n valeurs propres distinctes.

<u>$\Leftarrow$:</u> On suppose donc $r = n$ et donc u est diagonalisable. Il ne nous reste plus qu'à montrer que u est cyclique (*i.e.*) il existe $x \in E$ tel que $(x, u(x), ..., u^{n-1}(x))$ soit une base de E.
Soient x_i, pour $1 \leq i \leq n$, des vecteurs propres associés respectivement aux λ_i, pour $1 \leq i \leq n$. Montrons que $x = x_1 + ... + x_n$ convient.
Supposons qu'il existe une relation de dépendance linéaire pour $(x, u(x), ..., u^{n-1}(x))$, et donc un polynôme $P(X)$ de degré inférieur ou égal à $n - 1$ tel que $P(u)(x) = 0$. Or,

$$0 = P(u)(x) = P(u)(x_1) + ... + P(u)(x_n) = P(\lambda_1)x_1 + ... + P(\lambda_n)x_n$$

Comme les x_i forment une famille libre, alors on en déduit que pour tout $1 \leq i \leq n$, $P(\lambda_i) = 0$ et comme $\deg P \leq n - 1$, on a donc $P = 0$. Par conséquent, la relation de dépendance linéaire pour $(x, u(x), ..., u^{n-1}(x))$ est triviale et ainsi la famille $(x, u(x), ..., u^{n-1}(x))$ est libre (de cardinal n), et c'est donc une base de E.

Exercice : 1) Montrer le théorème de Maschke :
Toute représentation peut s'écrire comme somme de représentations irréductibles.
2) Montrer le lemme de Schur :
Soient ρ et ρ' deux représentations irréductibles d'un groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' et $f \in \mathcal{L}(V, V')$ un opérateur d'entrelacement. Alors
(i) Si ρ et ρ' ne sont pas isomorphes, alors $f = 0$.
(ii) Si $f \neq 0$, alors f est un isomorphisme.
Si on suppose $V = V'$, alors f est une homothétie.

Solution : 1) On raisonne par récurrence sur la dimension de V l'espace vectoriel de notre représentation.
Un espace de dimension 1 est irréductible.
Si V est un espace de dimension plus grande que 1 et irréductible, alors la démonstration est terminée.
Sinon, V admet un sous-espace stable non trivial W. Il nous faut donc trouver un supplémentaire stable W_0. En effet, une fois trouvé ces espaces W et W_0, on applique l'hypothèse de récurrence à ces sous-espaces. Ce qui prouvera le théorème.
On propose deux méthodes trouver un supplémentaire stable W_0.

<u>*Méthode 1 :*</u> Soit ρ une représentation de G sur V. Alors ρ laisse invariant le produit hermitien suivant :

$$\langle x, y \rangle_G := \sum_{g \in G} \langle \rho(g)(x), \rho(g)(y) \rangle$$

où $\langle ., . \rangle$ est un produit hermitien quelconque sur V.

En effet,

$$\begin{aligned}
\langle \rho(g)(x), \rho(g)(y) \rangle_G &:= \sum_{s \in G} \langle \rho(s)\rho(g)(x), \rho(s)\rho(g)(y) \rangle \\
&= \sum_{s \in G} \langle \rho(sg)(x), \rho(sg)(y) \rangle \\
&= \sum_{h \in G} \langle \rho(h)(x), \rho(h)(y) \rangle = \langle x, y \rangle_G
\end{aligned}$$

De plus, $\langle ., . \rangle_G$ est bien un produit hermitien comme somme de produits hermitiens.
En considérant donc ce produit hermitien, on peut prendre l'orthogonal de W, que l'on note W_0. Par conservation du produit scalaire, l'image par G d'un vecteur orthogonal à W est encore W : W_0 est donc bien stable sous l'action de G.

Méthode 2 : La deuxième méthode n'utilise pas le produit hermitien, et n'impose donc pas non plus que le corps soit $\mathbb{C}$. La démonstration qui suit est valable sur un corps K tel que sa caractéristique ne divise pas $|G|$.
Reprenons donc notre sous-espace stable W de V et considérons un supplémentaire quelconque (pas forcément stable !) W_1. Notons π la projection sur W associé à la décomposition $V = W \oplus W_1$. on définit ensuite l'endomorphisme

$$\pi_0 = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ \pi \circ \rho(g^{-1})$$

En fait, cet endomorphisme est un projecteur d'image W, et on a même $W_0 := \mathrm{Ker}\pi_0$ est un supplémentaire stable par l'action de G.

2)

Rappels :
• Soient ρ et ρ' deux représentations d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V'. Un opérateur d'entrelacement est une application linéaire $\tau : V \to V'$ tel que pour tout $g \in G$, $\tau \circ \rho(g) = \rho'(g) \circ \tau$

$$\begin{tikzcd}
V \arrow[r, "\tau"] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\
V \arrow[r, "\tau"] & V'
\end{tikzcd}$$

• On note $\mathrm{Hom}_G(V, V')$ l'ensemble des opérateurs d'entrelacements.
• Deux représentations ρ et ρ' d'un même groupe G respectivement sur deux $\mathbb{C}$-espace vectoriel V et V' sont dites isomorphes (ou G-isomorphes) si τ est bijective.

(i) Si on suppose que $f \neq 0$, alors $\mathrm{Ker}f$ est stable par tous les $\rho(g)$. En effet,

$$\forall x \in \mathrm{Ker}f, \quad f(\rho(g)(x)) = \rho'(g)(f(x)) = \rho'(g)(0) = 0$$

Ainsi, $\rho(g)(x) \in \mathrm{Ker}f$. Donc comme ρ est irréductible et $f \neq 0$, on en déduit que $\mathrm{Ker}f = \{0\}$. On montre de la même façon que $\mathrm{Im}f$ est stable par tous les $\rho'(g)$, et comme ρ' est irréductible et $f \neq 0$, on en déduit que $\mathrm{Im}f = V'$. Finalement, f est un isomorphisme, et ρ et ρ' sont isomorphes.

(ii) Comme V est un $\mathbb{C}$-e.v., f admet au moins une valeur propre. Par suite, on pose

$$f' = f - \lambda \mathrm{Id}$$

On remarque que $\mathrm{Ker}f' \neq \{0\}$ et en reprenant la première partie de la démonstration de la question précédente à f', on en déduit que $f' = 0$.