École Normale Supérieure de Rennes

AL3

ALGÈBRE LINÉAIRE
&
BILINÉAIRE

Espaces vectoriels, produits tensoriels, déterminant, réduction, espaces quadratiques, espaces euclidiens et hermitiens, représentation linéaire des groupes finis et théorie des caractères.

Auteur
Jérémy Leborgne

Notes de cours
Victor Lecerf

2020–2021

Table des matières

Chapitre 1

Espaces vectoriels et applications linéaires

Dans tout ce cours, $\mathbb{K}$ désignera un corps (commutatif, c'est mieux).

1.1 Espaces vectoriels

1.1.1 Définitions

Définition 1.1.1. *Un espace vectoriel sur le corps $\mathbb{K}$ (ou $\mathbb{K}$-espace vectoriel) est la donnée d'un triplet $(E, +, \cdot)$ où :*

— $(E, \cdot)$ *est un groupe abélien.*

— $\cdot : \mathbb{K} \times E \longrightarrow E$ *est une application distributive à gauche et à droite telle que pour tous* $\lambda, \mu \in \mathbb{K}$, $x, y \in E$,

- $1 \cdot x = x$;
- $\lambda\mu \cdot x = \lambda(\mu \cdot x)$.

Remarque. Un espace vectoriel est la donnée d'un groupe abélien $(E, +)$ et d'un morphisme d'anneaux $\mathbb{K} \longrightarrow \mathrm{End}_{gr}(E)$.

1.1.2 Sous-espaces vectoriels

Définition 1.1.2. *Soit E un $\mathbb{K}$-e.v, et $F \subset E$. On dit que F est un sous-espace vectoriel de E si $(F, +)$ est un sous-groupe de $(E, +)$ stable par la loi de composition externe.*

Proposition 1.1.1. *Soit E un $\mathbb{K}$-e.v, et $F \subset E$. F est un s.e.v de E si et seulement si 0_E est élément de F, et F est stable par combinaison linéaire.*

1.1.3 Familles remarquables et existence de base(s)

Définition 1.1.3. *Soit E un $\mathbb{K}$-e.v. Une famille $(x_i)_{i\in I}$ d'éléments de E est*

- ***libre*** *si toute combinaison linéaire nulle des éléments de cette famille a tous ses coefficients nuls ;*
- ***génératrice*** *si tout élément de E est combinaison linéaire d'éléments de cette famille ;*
- *une **base** si elle est libre et génératrice.*

Théorème 1.1.1. *Soit E un $\mathbb{K}$-e.v. Soient L une famille libre et G un famille génératrice de E telles que $L \subset G$. Alors il existe une base B de E telle que $L \subset B \subset G$.*

Démonstration. — *Cas fini.* Notons $L = (e_1, \dots, e_k)$ et $G = (e_1, e_2, \dots, e_k, e_{k+1}, \dots, e_m)$. Soit

$$n = \max\{\mathrm{card}(K) \mid [\![1,k]\!] \subset K \subset [\![1,m]\!] \text{ et} (e_i)_{i\in K} \text{ est libre.}\}$$

Soit K_0 associé à la définition de n. Soit $B = (e_i)_{i\in K_0}$, nous allons montrer que c'est une base. Elle est clairement libre, il faut donc montrer qu'elle est génératrice. G est génératrice : soit $x \in E$

$$x = \sum_{i=1}^{m} x_i e_i = \sum_{i\in K_0}^{m} x_i e_i + \sum_{i\notin K_0}^{m} x_i e_i$$

Soit $i \notin K_0$, alors $\mathrm{card}(B \cup \{e_i\}) = n + 1 > n$, et $B \cup \{e_i\}$ est incluse dans G. Par définition de n, $B \cup \{e_i\}$ est nécessairement liée. Donc e_i est combinaison linéaire d'éléments de B. Donc B génère E puisqu'elle génère tous les éléments de G.

— *Cas général.* Dans cette démonstration, nous considérerons les familles comme des parties de E. Soit A_L l'ensemble des parties libres de E contenant L. Montrons alors que l'ensemble ordonné $(A_L, \subset)$ est inductif : soit $(L_i)_{i\in I}$ une famille de parties libres de V incluant L, telles que pour tout $i, j \in I$, on $L_i \subset L_j$ ou $L_j \subset L_i$. Soit $L' = \cup_{i\in I} L_i$. Montrons que L' est libre. Soit $\{e_k \mid k \in [\![1,n]\!]\}$ une famille finie d'éléments de L', et soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ telle que

$$\sum_{k=1}^{n} \lambda_k e_k = 0.$$

Pour tout $k \in [\![1,n]\!]$, il existe un indice i_k tel que $e_k \in L_{i_k}$. Or, les L_{i_k} sont deux à deux comparables, ce qui impose qu'il existe un $i \in I$ tel que L_i contient tous les L_{i_k}. Or, puisque que L_i est libre, on a nécessairement $\lambda_k = 0$ pour tout $k \in [\![1,n]\!]$. On en déduit que L' est une partie libre de la chaine $(L_i)_{i\in I}$. On peut alors appliquer le lemme de Zorn : soit B un élément maximal dans $(A_L, \subset)$. Par construction, B est une partie libre dans E qui contient L et telle que toute partie contenant B strictement n'est pas libre. Soit maintenant $e \in V \backslash B$. Puisque la famille $B \cup \{e\}$ n'est pas libre, il existe $(\lambda_1, \dots, \lambda_m, \lambda) \in \mathbb{K}^{m+1}$ une famille non nulle de scalaires telle que

$$\lambda e + \sum_{k=1}^{m} \lambda_k e_k = 0.$$

On remarque alors que λ est non nul (si c'était le cas, la liberté de B imposerait que $\lambda_k = 0$ pour tout $k \in [\![1, m]\!]$). On en déduit que λ est non nul et que

$$e = -\sum_{k=1}^{m} \frac{\lambda_k}{\lambda} e_k.$$

Cela montre alors que B est aussi une partie génératrice de E. C'est donc une base.

□

Remarque. Dans la démonstration du cas général (hors-programme en L3), nous avons uniquement démontré l'existence d'une base de E contenant L. Cependant, l'argument s'adapte facilement à l'énoncé exact du théorème en considérant $(A_{L,G}, \subset)$, l'ensemble ordonné des parties F de $G \backslash L$ telles que $L \cup F$ est libre.

Proposition 1.1.2. *Les bases d'un espace vectoriel donné sont de même cardinal, appelé dimension de E.*

1.1.4 Sommes de sous-espaces

Définition 1.1.4. *Soit $E_1, \ldots, E_p \subset E$ des s.e.v de E. L'image de l'application linéaire*

$$\begin{array}{ccc} E_1 \times \cdots \times E_p & \longrightarrow & E \\ (x_1, \ldots, x_p) & \longmapsto & \displaystyle\sum_{i=1}^{p} x_i \end{array}$$

est appelée la somme des espaces E_i, notée $\sum_{i=1}^{p} E_i$. Si elle est injective, la somme est dite directe, et est notée

$$\bigoplus_{i=1}^{p} E_i$$

1.2 Applications linéaires

Définition 1.2.1. *Soient E et F des $\mathbb{K}$-e.v, une application $u : E \longrightarrow F$ est dite linéaire si*

$$\forall (x, y) \in E^2, \forall \lambda \in \mathbb{K}, u(x + \lambda y) = u(x) + \lambda u(y)$$

On note $\mathscr{L}(E, F)$ l'espace vectoriel des ces telles applications (ou $\mathscr{L}(E)$ quand $E = F$).

Définition 1.2.2. *Soit $u : E \longrightarrow F$ une application linéaire. On note*

$$\ker u = u^{-1}(0_F) \text{ et } \operatorname{Im} u = u(E)$$

Ce sont des sous-espaces vectoriels, respectivement de E et de F. On appelle rang de u la dimension de $\operatorname{Im} u$.

Remarque. Plus généralement, pour tout s.e.v G de F, $u^{-1}(G)$ est un s.e.v de E.

Théorème 1.2.1. *Toute application linéaire de E dans F est uniquement déterminée par l'image d'une base donnée.*

Démonstration. Soit $\mathcal{B} = (e_i)_{i\in I}$ une base de E. Soit $u \in \mathscr{L}(E, F)$ et $x \in E$. Il existe une famille de scalaires $(\lambda_i)_{i\in I}$ à support fini telle que

$$x = \sum_{i\in I} \lambda_i e_i.$$

On a alors par linéarité (car la somme est finie) que

$$u(x) = \sum_{i\in I} \lambda_i u(e_i).$$

D'où le résultat.

□

1.3 Espace vectoriel quotient

Définition 1.3.1. *Soit E un $\mathbb{K}$-e.v, F un s.e.v de E. On appelle espace quotient E/F l'ensemble des classes d'équivalences des éléments de E par la relation d'équivalence définit par*

$$x\mathscr{R}y \iff x - y \in F$$

On appelle projection (ou surjection) canonique l'application $\pi : E \longrightarrow E/F$ qui à tout élément de E lui associe sa classe d'équivalence par la relation $\mathscr{R}$.

Proposition 1.3.1. *Il existe une unique structure d'espace vectoriel sur E/F telle que π soit linéaire.*

Démonstration. Si l'on suppose trouvée une telle structure sur E/F, alors pour tout $x, y \in E$ et $\lambda \in \mathbb{K}$, $\pi(x + \lambda y) = \pi(x) + \lambda\pi(y)$, ce qui décrit entièrement cette structure car π est surjective. Il suffit donc de montrer que cette dite structure est bien définie. Soit $x_1, x_2, y_1, y_2 \in E$ tels que $\pi(x_1) = \pi(x_2)$ et $\pi(y_1) = \pi(y_2)$. D'une part, on sait que $x_1 + y_1 - (x_2 + y_2) \in F$ car $x_1 - x_2$ et $y_1 - y_2 \in F$, d'où $\pi(x_1 + y_1) = \pi(x_2 + y_2)$. On montre de la même manière que pour tout $\lambda \in \mathbb{K}$, $\pi(\lambda x_1) = \pi(\lambda x_2)$.

□

Proposition 1.3.2. *Soit E et G des $\mathbb{K}$-e.v, F un s.e.v de E. Si $F \subset \ker u$, alors il existe unique application linéaire $\tilde{u} : E/F \longrightarrow G$ telle que $u = \tilde{u} \circ \pi$.*

Démonstration. Supposons trouvée une telle application $\tilde{u}$. On remarque en particulier que cette dernière est entièrement déterminée puisque $u = \tilde{u} \circ \pi$. Montrons qu'elle est bien définie. Soient x et x' tels que $\pi(x) = \pi(x')$. Alors, $x - x' \in F$ donc $u(x - x') = 0_G$ et $u(x) = u(x')$. Ainsi, deux éléments de la même classe d'équivalences ont même images par u. Ainsi, on peut définir $\tilde{u}(x)$ telle que $u(x) = \tilde{u}(\pi(x))$. Cette expression a du sens puisque l'image par u de x ne dépend que de sa classe d'équivalence dans E/F. Soient maintenant $\overline{x}, \overline{y} \in E/F$ représentés respectivement par x et $y \in E$. Soit $\lambda \in \mathbb{K}$. Alors,

$$\begin{aligned} \tilde{u}(\overline{x} + \lambda\overline{y}) &= \tilde{u}(\pi(x) + \lambda\pi(y)) \\ &= \tilde{u}(\pi(x + \lambda y)) \\ &= u(x + \lambda y) \\ &= u(x) + \lambda u(y) \\ &= \tilde{u}(\overline{x}) + \lambda\tilde{u}(\overline{y}) \end{aligned}$$

D'où la linéarité de $\tilde{u}$.

□

Corollaire 1.3.1 (Premier théorème d'isomorphisme)**.** *Soit E et G des $\mathbb{K}$-e.v, $u \in \mathscr{L}(E, G)$. Alors $E/\ker u \cong \operatorname{Im} u$.*

Démonstration. Montrons que $\tilde{u} : E/\ker u \longrightarrow G$ est un isomorphisme. Soit $y \in \operatorname{Im}(u)$, notons $y = u(x)$, alors la classe d'équivalence de x convient comme antécédent. Soit maintenant $\overline{x} \in \ker \tilde{u}$ (où x est un représentant de cette classe d'équivalence). Par la proposition précédente, $\tilde{u}(\overline{x}) = u(x)$, donc $x \in \ker u$. Cela signifie que x est dans la même classe d'équivalence que 0_E, donc $\overline{x} = \pi(x) = \pi(0_E) = 0_{E/\ker u}$.

□

Proposition 1.3.3. *Soit E un $\mathbb{K}$-e.v, et $F \subset E$ un sous-espace vectoriel. Alors :*

$$\dim E/F + \dim F = \dim E$$

Démonstration. Justifions d'abord que le résultat garde son sens en dimension infinie. L'application π étant surjective, l'image par π d'une famille génératrice d'éléments de E est une famille génératrice dans E/F, donc $\dim E \geq \dim E/F$. De plus, toute famille libre dans F l'est aussi dans E, d'où $\dim F \leq \dim E$. Supposons maintenant F et E/F de dimensions finies. Soit $(f_1, \ldots, f_k)$ une base de F, et $(\gamma_1, \ldots, \gamma_m)$ une base de E/F. Soit $x \in E$, alors il existe une famille $(\lambda_1, \ldots, \lambda_m) \in \mathbb{K}^m$ telle que

$$\pi(x) = \sum_{i=1}^{m} \lambda_i \gamma_i.$$

Par surjectivité de π, il existe $g_1, \ldots, g_m$ des antécédents respectifs de $\gamma_1, \ldots, \gamma_m$. On a alors que

$$\pi\left(x - \sum_{i=1}^{m} \lambda_i g_i\right) = 0_{E/F}$$

Ainsi, $x - \sum_{i=1}^{m} \lambda_i g_i \in F$. Il existe alors $\mu_1, \ldots, \mu_k \in \mathbb{K}$ tels que

$$x = \sum_{i=1}^{m} \lambda_i g_i + \sum_{j=1}^{k} \mu_j f_j.$$

La famille $(g_1, \ldots, g_m, f_1, \ldots, f_k)$ est bien génératrice. Il suffit de vérifier qu'elle est libre. Soient $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_m \in \mathbb{K}$ tels que

$$\sum_{i=1}^{m} \lambda_i g_i + \sum_{j=1}^{k} \mu_j f_j = 0_E.$$

Avec π, on obtient que

$$0_{E/F} = \sum_{i=1}^{m} \lambda_i \gamma_i$$

La famille $(\gamma_1, \ldots, \gamma_m)$ étant libre dans E/F, les λ_i sont tous nuls. Enfin, les μ_j le sont aussi car on obtient

$$\sum_{j=1}^{k} \mu_j f_j = 0_E,$$

mais la famille $(f_1, \ldots, f_k)$ est libre dans E.

□

Théorème 1.3.1 (du rang)**.** *Soit $u : E \longrightarrow E'$ une application linéaire. Alors :*

$$\dim E = \dim \ker u + \operatorname{rg} u$$

Démonstration. Appliquer le résultat précédent avec $F = \ker u$.

□

Corollaire 1.3.2. *Soit E et E' des $\mathbb{K}$-e.v, et $u \in \mathscr{L}(E, E')$. On suppose E et E' de dimension finie avec $\dim E = \dim E'$. Sont équivalents :*

(i) u est injective.

(ii) u est surjective.

(iii) u est un isomorphisme.

Démonstration. Si u est injective, alors $\dim \ker u = 0$ et donc $\operatorname{rg} u = \dim E$, donc $\operatorname{Im}(u) = E$ et u est surjective. Si u est surjective, on en déduit de même que $\ker u = \{0_E\}$.

□

1.4 Dualité

1.4.1 Espace dual

Définition 1.4.1. *Soit E un $\mathbb{K}$-e.v. On appelle espace vectoriel dual de E l'espace des formes linéaires sur E,*

$$E^* = \mathscr{L}(E, \mathbb{K}).$$

Définition 1.4.2. *Soient* E, F *des* $\mathbb{K}$*-e.v, et* $u \in \mathscr{L}(E, F)$*. Il existe un unique* ${}^t u \in \mathscr{L}(F^*, E^*)$ *tel que pour tout* $\phi \in E^*$, ${}^t u(\phi) = \phi \circ u$ *: c'est le transposé de* u*.*

Exercice. Déterminer en dimensions finies la matrice de ${}^t u$ en fonction de celle de u dans une base donnée.

Proposition 1.4.1. *Soit* E *un* $\mathbb{K}$*-e.v de dimension finie, et* $\mathcal{B} = (e_i)_{1 \leq i \leq n}$*. Alors la famille* $(e_i^*)_{1 \leq i \leq n} \in (E^*)^n$ *définie par :*

$$\forall i, j \in [\![1, n]\!],\ e_i^*(e_j) = \delta_{i,j}$$

est une base de E^**. C'est la base duale associée à* $\mathcal{B}$*.*

Corollaire 1.4.1. *En dimension finie,* $\dim E = \dim E^*$*.*

Remarques. Résultat faux en dimension finie : $\mathbb{K}[X]^* \cong \mathbb{K}^{\mathbb{N}}$. De plus, si l'espace n'est pas euclidien, on n'a pas nécessairement d'isomorphisme canonique.

1.4.2 Orthogonalité

Définition 1.4.3. *Soit* A *une partie quelconque de* E*. On appelle orthogonal de* A *pour la dualité l'ensemble des formes linéaires qui s'annulent sur* A *:*

$$A^o = \{\phi \in E^* \,|\, \forall x \in A,\ \phi(x) = 0\}$$

Proposition 1.4.2. *Soit* E *un* $\mathbb{K}$*-e.v de dimension finie. Soit* $A \subset E$*. Alors :*

$$\dim E = \dim \mathrm{Vect}(A) + \dim A^o$$

Remarque. Si un sous-espace F est stable par $u \in \mathscr{L}(E)$, alors F^o est stable par ${}^t u$.

1.4.3 Espace bidual

Théorème 1.4.1. *Soit* E *un* $\mathbb{K}$*-e.v de dimension finie. Alors l'application :*

$$\begin{array}{ccc} E & \longrightarrow & E^{**} \\ x & \longmapsto & \left(\begin{array}{cccc} f_x : & E^* & \longrightarrow & \mathbb{K} \\ & \phi & \longmapsto & \phi(x) \end{array} \right) \end{array}$$

est un isomorphisme.

Chapitre 2

Produits tensoriels, matrices, puissances extérieures

2.1 Produit tensoriel d'espaces vectoriels

2.1.1 Applications bilinéaires

Définition 2.1.1 (Application bilinéaire)**.** *Soient E, F et G des $\mathbb{K}-e.v.$ Une application $B : E \times F \longrightarrow G$ est une application dite* ***bilinéaire*** *si $B(\,\cdot\,, y)$ est linéaire pour tout $y \in F$, et $B(x, \,\cdot\,)$ est linéaire pour tout $x \in E$.*

Théorème 2.1.1 (Propriété universelle du produit tensoriel)**.** *Soient E,F des $\mathbb{K}$-e.v. Il existe un espace vectoriel noté $E \otimes F$ ainsi qu'une application bilinéaire $\cdot \otimes \cdot$ tels que pour tout $\mathbb{K}$-e.v G et toute application bilinéaire $b : E \times F \to G$, il existe une unique application linéaire $\widetilde{b} : E \otimes F \to G$ de sorte que :*

$$\forall (x, y) \in E \times F,\, b(x, y) = \widetilde{b}(x \otimes y)$$

On décompose ainsi toute application bilinéaire en deux applications linéaires.

Démonstration. Intéressons nous à l'espace $\mathbb{K}^{(E\times F)} =: H$. Notons pour tout $(x, y) \in E \times F$: $[x, y] = \mathbb{1}_{(x,y)}$. Soit T le s.e.v de $\mathbb{K}^{(E\times F)}$ engendré par les éléments de la forme :

- $[x + x', y] - [x, y] - [x', y]$
- $[x, y + y'] - [x, y] - [x, y']$
- $\lambda[x, y] - [\lambda x, y]$
- $\lambda[x, y] - [x, \lambda y]$

pour les $(x, y), (x', y') \in E \times F$, et $\lambda \in \mathbb{K}$. On définit ensuite $E \otimes F := H/T$, et $x \otimes y$ comme la classe d'équivalence de $[x, y]$ dans ce groupe quotient.

Soit $b : E \times F \to G$ une application bilinéaire. On peut identifier $E \times F$ à la base "canonique"[1] de $\mathbb{K}^{(E\times F)}$. Ainsi, on définit un "prolongement"[2] de b dans l'espace H. On pose :

1. ...I guess?
2. J'aime pas dire ça, mais bon.

$$\forall (x,y) \in E \times F,\ B([x,y]) = b(x,y)$$

B est bien définie car c'est une application linéaire définie sur une base de H. Montrons alors que $T \subset \ker(B)$. Soit $(x,y),(x',y') \in E \times F$, et $\lambda \in \mathbb{K}$, alors :

$$\begin{aligned} B([x+x',y]-[x,y]-[x',y]) &= B([x+x',y]) - B([x,y]) - B([x',y]) \\ &= b(x+x',y) - b(x,y) - b(x',y) = b(0_E,y) \\ &= 0_G \end{aligned}$$

On vérifie de même pour les trois autres types de fonctions. En utilisant alors la factorisation avec la projection canonique de $H/T = E \otimes F$, on sait qu'il existe une unique application bilinéaire $\tilde{b} : E \otimes F \to G$ vérifiant :

$$\forall (x,y) \in E \otimes F,\ \tilde{b}(x \otimes y) = B(x,y) = b(x,y)$$

[3]

Cette application est bien unique car $E \otimes F = \{x \otimes y \,|\, (x,y) \in E \times F\}$.

□

Proposition 2.1.1. *Soient E, E', F, F' des $\mathbb{K}$-e.v. Soient $u : E \longrightarrow E'$, et $v : F \longrightarrow F'$ des applications linéaires. Il existe une unique application linéaire $u \otimes v : E \otimes F \longrightarrow E' \otimes F'$ telle que :*

$$\forall (x,y) \in E \times F,\ (u \otimes v)(x \otimes y) = u(x) \otimes v(y)$$

Démonstration. Soit $b : E \times F \longrightarrow E' \otimes F'$, $(x,y) \longmapsto u(x) \otimes v(y)$, elle est bilinéaire donc il existe une unique application bilinéaire $\tilde{b} : E \otimes F \longrightarrow E' \otimes F$ telle que pour tous $(x,y) \in E \times F$,

$$\tilde{b}(x \otimes y) = b(x,y) = u(x) \otimes v(y)$$

$\tilde{b}$ convient et est unique.

□

Proposition 2.1.2. *Soient E et F des $\mathbb{K}$-e.v. Soit $(e_i)_{i \in I}$ base de E, et $(f_j)_{j \in J}$ base de F. Alors $(e_i \otimes f_j)_{(i,j) \in I \times J}$ est une base de $E \otimes F$. De plus, lorsque E et F sont de dimensions finies, $E \otimes F$ est aussi de dimension finie* $\dim E \otimes F = \dim E \cdot \dim F$.

Démonstration. Montrons que cette famille est génératrice. Soit $x = \sum_{i \in I} x_i e_i$, et $y = \sum_{j \in J} y_j e_j$. Alors par bilinéarité :

$$x \otimes y = \sum_{i,j \in I \times J} x_i y_j (e_i \otimes f_j)$$

Soit désormais $\alpha_{i,j \in I \times J}$ une famille de scalaires telle que $\sum_{i,j} \alpha_{i,j}(e_i \otimes f_j) = 0$. Soient $(k,l) \in I \times F$, on pose $\phi_{k,l} = e_k * \otimes f_j *$. Alors :

3. $\tilde{u} = \pi \circ u$

$$\begin{aligned} 0 &= \sum_{i,j} \alpha_{i,j} \phi_{k,l}(e_i \otimes f_j) \\ &= \sum_{i,j} \alpha_{i,j} (e_k^*(e_i) \otimes f_k^*(f_j)) \\ &= \alpha_{k,l}(1 \otimes 1) \end{aligned}$$

Puisque $\mathbb{K} \otimes \mathbb{K} \longrightarrow \mathbb{K}$, $\lambda \otimes \mu \longmapsto \lambda\mu$ est un isomorphisme, on a nécessairement $\alpha_{k,l} = 0$, et ce pour tout $(k,l) \in I \times J$.

□

Corollaire 2.1.1. *Soient E, F des $\mathbb{K}-e.v.$ On a :*

$$(E \otimes F)^* \cong E^* \otimes F^*$$

Proposition 2.1.3. *Soient E, F et G des $\mathbb{K}-e.v.$ Il existe un unique isomorphisme de $\mathbb{K}$-e.v*

$$\theta : (E \otimes F) \otimes G = E \otimes (F \otimes G)$$

tel que :

$$\forall (x,y,z) \in E \times F \times G,\ \theta((x \otimes y) \otimes z) = \theta(x \otimes (y \otimes z))$$

2.2 Matrices

2.2.1 Matrices et applications linéaires

Proposition 2.2.1. *Soit $\mathbb{A}$ un anneau unitaire commutatif. Alors $(\mathcal{M}_{m,n}(\mathbb{A}), +)$ est un groupe. Si $\mathbb{A}$ est un corps, c'est alors un $\mathbb{A}$-e.v de dimension nm.*

Définition 2.2.1. *Soit m, n, p des entiers. On définit le produit de deux matrices $A = (a_{i,j})_{i,j} \in \mathcal{M}_{m,n}(\mathbb{K})$ et $B = (b_{i,j})_{i,j} \in \mathcal{M}_{n,p}(\mathbb{K})$ comme la matrice :*

$$AB = \left(\sum_{k=1}^{n} a_{i,k} b_{k,j} \right)_{i,j} \in \mathcal{M}_{m,p}(\mathbb{K})$$

Définition 2.2.2. *Soient E et F des $\mathbb{K}$-e.v de dimension finie. Soit $\mathcal{B}_E = (e_1, \ldots, e_n)$ et $\mathcal{B}_F = (f_1, \ldots, f_p)$ des bases respectives de E et de F. Soit $u \in \mathscr{L}(E,F)$. Soit $i \in [\![1, n]\!]$, on note $u(e_i) = \sum_{j=1}^{p} m_{i,j} f_j$.On appelle matrice de u dans les bases $\mathcal{B}_E$, $\mathcal{B}_F$ la matrice :*

$$\mathrm{mat}_{\mathcal{B}_E, \mathcal{B}_F}(u) = (m_{i,j})_{i,j} \in \mathcal{M}_{p,n}(\mathbb{K})$$

Proposition 2.2.2. *L'application :*

$$\begin{array}{rcl} \mathscr{L}(E,F) & \longrightarrow & \mathcal{M}_{p,n}(\mathbb{K}) \\ u & \longmapsto & \mathrm{mat}_{\mathcal{B}_E,\mathcal{B}_F}(u) \end{array}$$

est un isomorphisme de groupe. Si $E = F$, c'est même un isomorphisme d'algèbre.

2.2.2 Évaluation en application linéaire

Soit $x \in E$ un espace vectoriel de dimension finie, $\mathcal{B} = (e_1, \dots, e_n)$ une base. On note $x = \sum_{i=1}^n x_i e_i$. On appelle matrice de x dans la base B la matrice :

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{K})$$

Qu'on identifiera souvent à un vecteur de $\mathbb{K}^n$.

2.2.3 Changement de base

Définition 2.2.3. *Soit $\mathcal{B}_1, \mathcal{B}_2$ deux bases d'un espace vectoriel de dimension finie. On appelle matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$ la matrice :*

$$P_{B_1}^{B_2} = \mathrm{mat}_{\mathcal{B}_2,\mathcal{B}_1}(\mathrm{id}_E)$$

2.3 Puissances extérieures

2.3.1 Applications multilinéaires

Définition 2.3.1. *Soit $n \in \mathbb{N}^*$,E, F des $\mathbb{K}$-e.v, et $f : E^n \longrightarrow F$ une application n-linéaire. f est dite alternée si pour tous $(x_1, \dots x_n) \in E^n$.*

$$\big(\exists i, j \in [\![1, n]\!],\, (i \neq j) \wedge (x_i = x_j)\big) \Longrightarrow \big(f(x_1, \dots, x_n) = 0_F\big)$$

Proposition 2.3.1. *Soit $f : E^n \longrightarrow F$ multilinéaire alternée. Soit $(x_1, \dots, x_n) \in E^n$, et $\sigma \in \mathfrak{S}_n$. Alors :*

$$f(x_1, \dots, x_n) = \varepsilon(\sigma) f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

En particulier (pour les transpositions), f est antisymétrique. La réciproque est vrai lorsque la caractéristique du corps est différente de 2.

2.3.2 Puissance extérieure

Soit $r \in \mathbb{N}^*$. Notons S_r le s.e.v de $E \otimes \cdots \otimes E$ généré par les éléments de la forme $x_1 \otimes \cdots \otimes x_r$ tels qu'il existe $i \neq j$ des entiers tels que $x_i = x_j$. On va pouvoir construire un espace vectoriel sur lequel les applications multilinéaires vont s'annuler.

Lemme 2.3.1. *Soit $f : E^r \longrightarrow F$. Alors f est alternée si et seulement si l'application induite par f sur $E^{\otimes r}$ est nulle sur S_r.*

On définit la r-ième puissance extérieur $\bigwedge^r(E) = E^{\otimes r}/S_r$. On note $x_1 \wedge \cdots \wedge x_r$ la classe d'équivalence de $x_1 \otimes \cdots \otimes x_r$ dans ce quotient.

Proposition 2.3.2. *Il existe un isomorphisme naturel entre l'espace des applications r-linéaires de E^r dans F, et $\mathscr{L}(\bigwedge^r E, F)$.*

Théorème 2.3.1. *Soit E un $\mathbb{K}$-e.v de dimension $n \in \mathbb{N}^*$, et $(e_1, \ldots, e_n)$ une base de E. Une base de $\bigwedge^r E$ est donnée par les éléments de la forme $e_{i_1} \wedge \cdots \wedge e_{i_r}$, où $1 \leq i_1 < \cdots < i_r \leq n$.*

On suppose que la caractéristique de $\mathbb{K}$ est différente de 2.

Corollaire 2.3.1. *Soit E un $\mathbb{K}$-e.v de dimension $n \in \mathbb{N}^*$. Alors :*

$$\dim \bigwedge^r E = \binom{n}{r}$$

Corollaire 2.3.2. *Soit E un $\mathbb{K}$-e.v de dimension $n \in \mathbb{N}^*$, et $(e_1, \ldots, e_n)$ une base de cette espace. La base duale $(e_I^*)_{|I|=r}$ de $(\bigwedge^r E)^*$ est donnée par la formule :*

$$e_I^*(x_1 \wedge \cdots \wedge x_r) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} e_i^*(x_{\sigma(i)})$$

2.3.3 Déterminant

Constructions

Définition 2.3.2 (Déterminant)**.** *Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E et $x_1, \ldots, x_n$ une famille d'éléments de E. On appelle déterminant en base $\mathcal{B}$ de la famille $(x_1, \ldots, x_n)$ l'unique scalaire $\det_{\mathcal{B}}(x_1, \ldots, x_n)$ tel que*

$$x_1 \wedge \cdots \wedge x_n = \det_{\mathcal{B}}(x_1, \ldots, x_n)(e_1 \wedge \cdots \wedge e_n)$$

Définition 2.3.3. *Soit $u \in \mathscr{L}(E, F)$. On définit $\bigwedge^r u : \bigwedge^r E \longrightarrow \bigwedge^r F$ par :*

$$\bigwedge^r u(x_1 \wedge \cdots \wedge x_r) = (u(x_1) \wedge \cdots \wedge u(x_r))$$

Définition 2.3.4. *Soit E un $\mathbb{K}$-e.v de dimension n et $u \in \mathscr{L}(E)$. On définit le déterminant d'un endomorphisme comme le rapport de l'homothétie $\bigwedge^n u$ dans $\bigwedge^n E$ (qui est un espace de dimension 1).*

Lemme 2.3.2. *Soient $u : E \longrightarrow F$ et $v : F \longrightarrow G$, et $r \in \mathbb{N}$. Alors :*

$$\bigwedge^r (v \circ u) = \bigwedge^r v \circ \bigwedge^r u$$

Si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de E, il existe une unique forme n-linéaire alternée valant 1 en $\mathcal{B}$. On l'appelle le *déterminant en base* $\mathcal{B}$, noté $\det_{\mathcal{B}}$.

Lemme 2.3.3. *Soit $(x_1, \dots, x_r) \in E^r$. Si la famille $(x_1, \dots, x_r)$ est liée, alors :*

$$x_1 \wedge \cdots \wedge x_r = 0_{\bigwedge^r E}$$

Proposition 2.3.3. *Soit E un $\mathbb{K}$-e.v de dimension $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in E^n$, et $\mathcal{B}$ une base de E. Sont équivalents :*

i. $\det_{\mathcal{B}}(x_1, \dots, x_n) \neq 0$

ii. $x_1 \wedge \cdots \wedge x_n \neq 0_{\bigwedge^n E}$

iii. $(x_1, \dots, x_n)$ *est une base de* E.

Proposition 2.3.4. *Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. Alors :*

$$\det(u) = \det_{\mathcal{B}}(u(e_1), \dots, u(e_n))$$

Propriétés

Définition 2.3.5. *Soit $M \in \mathcal{M}_n(\mathbb{K})$, et u l'endomorphisme canoniquement associé à M. On définit* $\det(M) = \det(u)$.

Proposition 2.3.5. *L'application* $\det : \big(\mathcal{M}_n(\mathbb{K}), \times\big) \longrightarrow (\mathbb{K}, \cdot)$ *est un morphisme de groupes.*

En conséquence, deux matrices semblables ont même déterminant.

2.3.4 Comatrice

Définition 2.3.6. *Soit $M \in \mathcal{M}_n(\mathbb{K})$, $(i, j) \in [\![1, n]\!]$. On appelle cofacteur d'indice (i, j) le déterminant de la matrice obtenue en ôtant la i-ième ligne et la j-ième colonne de M, qu'on note $c_{i,j}(M)$.*
On appelle comatrice de M la matrice $\big((-1)^{i+j} c_{i,j}(M)\big)_{i,j \in [\![1,n]\!]}$.

Proposition 2.3.6. *Soient E et E' est $\mathbb{K}$-e.v de dimensions finies munis respectivement des bases (e_i) et (f_j). Soit $u \in \mathscr{L}(E)$ de matrice M dans les bases précédentes. Alors les coefficient de la matrice $\Lambda^p u$ dans les bases associées (e_I) et (f_J) sont les mineurs de taille p de M.*

Corollaire 2.3.3. *L'application linéaire $u \in \mathscr{L}(E, E')$ est de rang au plus $p-1$ si et seulement si tous les mineurs de taille p de sa matrice sont nuls.*

Proposition 2.3.7 (Formule de Binet-Cauchy)**.** *Soient $A \in \mathcal{M}_{n,m}(\mathbb{K})$, $B \in \mathcal{M}_{m,n}(\mathbb{K})$. Pour $J \subset [\![1, m]\!]$, on note A_J (resp. B_J) la matrice extraite de A (resp. B) en conservant les colonnes (resp. les lignes) dont les indices sont dans J. On a alors le résultat :*

$$\det(AB) = \sum_{|J|=n} \det(A_J)\det(B_J)$$

Proposition 2.3.8. *Soit $M \in \mathcal{M}_n(\mathbb{K})$. On a :*

$${}^t\mathrm{com}(M)M = \det(M)I_n$$

2.4 Calcul matriciel

2.4.1 Actions naturelles sur les espaces de matrices

On dispose d'une action naturelle de $\mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ sur $\mathcal{M}_{n,m}(\mathbb{K})$:

$$(P, Q) \cdot M = PMQ^{-1}$$

Définition 2.4.1. *Deux matrices d'une même orbite pour cette action sont dites **équivalentes**.*

On en déduit donc une action naturelle de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$:

$$P \cdot M = PMP^{-1}$$

Définition 2.4.2. *Deux matrices d'une même orbite pour cette action sont dites **semblables**.*

Proposition 2.4.1. *Soient $M, N \in \mathcal{M}_{m,n}(\mathbb{K})$, $u \in \mathscr{L}(\mathbb{K}^n, \mathbb{K}^m)$ l'application canoniquement associée à M. Alors N est équivalente à M si et seulement si il existe des des bases $\mathcal{B}, \mathcal{B}'$ des bases respectives de $\mathbb{K}^n$ et $\mathbb{K}^m$ telles que $N = \mathrm{mat}_{\mathcal{B},\mathcal{B}'}(u)$.*

Proposition 2.4.2. *Soit $M \in \mathcal{M}_{m,n}(\mathbb{K})$, alors M est équivalente à une unique matrice de la forme :*

$$\left(\begin{array}{c|c} I_r & (0)_{r,n-r} \\ \hline (0)_{m-r,r} & (0)_{m-r,n-r} \end{array}\right)$$

Où r est le rang de la matrice M.

Corollaire 2.4.1. *Deux matrices de mêmes dimensions sont équivalentes si et seulement si elles ont le même rang.*

Chapitre 3

Déterminant, polynômes d'endomorphismes

3.1 Polynômes d'endomorphismes

Soit E un $\mathbb{K}$-e.v de dimension finie, et $u \in \mathscr{L}(E)$.

Proposition 3.1.1. *Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre, et $a \in \mathbb{A}$. L'application*

$$\begin{array}{rccc} \varepsilon_a : & \mathbb{K}[X] & \longrightarrow & \mathbb{A} \\ & X & \longmapsto & a \end{array}$$

est bien définie, et est un morphisme d'algèbres. On note $P(a)$ pour $\varepsilon_a(P)$.

On peut donc considérer pour tous polynômes $P \in \mathbb{K}[X]$ l'endomorphisme $P(u)$. On note $\mathbb{K}[u]$ l'image de $\mathbb{K}[X]$ par ε_u.

Définition 3.1.1 (Sous-espace stable)**.** *Soit F un sous-espace vectoriel de E. F est dit **stable** par u si $u(F) \subset F$.*

Définition 3.1.2 (Endomorphisme induit)**.** *Soit F un sous-espace vectoriel de E stable par u. On appelle endomorphisme induit par u sur F l'endormorphisme $u_{|F} \in \mathscr{L}(F)$.*

Lemme 3.1.1 (Lemme des noyaux)**.** *Soit $P_1, \ldots, P_r \in \mathbb{K}[X]$ des polynômes premiers entre eux. Alors :*

$$\ker(P_1 \cdots P_r(u)) = \bigoplus_{i=1}^{r} \ker(P_i(u))$$

Démonstration. Démontrons le résultat pour le cas $r = 2$, il pourra alors servir à une démonstration par récurrence. Soient P_1 et P_2 des polynômes premiers entre eux de $\mathbb{K}[X]$. Il existe donc $(A, B) \in \mathbb{K}[X]^2$ tels que $AP_1 + BP_2 = 1$.

— Soit $x \in \ker(P_1P_2(u))$. Selon la relation : $x = \underbrace{(AP_1)(x)}_{\in \ker(P_2(u))} + \underbrace{(BP_2)(x)}_{\in \ker(P_1(u))}$. L'inclusion réciproque est claire.

— Soit $x \in \ker(P_1(u)) \cap \ker(P_2(u))$. Toujours avec la relation : $x = (AP_1)(x) + (BP_2)(x) = 0_E$.

□

Définition 3.1.3 (Polynôme annulateur)**.** *Un polynôme $P \in \mathbb{K}[X]$ est dit **annulateur** de u si $P(u) = 0_{\mathscr{L}(E)}$.*

Lemme 3.1.2. *$\mathcal{I}(u) = \{P \in \mathbb{K}[X] \,|\, P(u) = 0_{\mathscr{L}(E)}\}$ est un idéal non nul de $\mathbb{K}[X]$. Puisque $\mathbb{K}[X]$ est principal, il existe un unique polynôme unitaire π_u tel que $\mathcal{I}(u) = (\pi_u)$.*

Remarque. Sans l'hypothèse de dimension finie, l'existence d'un polynôme annulateur n'est pas assurée. En dimension finie, ce dernier existe car ε_u ne peut-être injective puisque $\mathbb{K}[X]$ est de dimension infinie.

Définition 3.1.4 (Valeur propre, vecteur propre)**.** *Soit E un $\mathbb{K}$-e.v. Soit $\lambda \in \mathbb{K}$, et $u \in \mathscr{L}(E)$. λ est appelée valeur propre si l'endomorphisme $u - \lambda\,\mathrm{id}_E$ n'est pas injectif. Son noyau est noté $E_\lambda(u)$, et une élément du noyau est appelé vecteur propre associé à la valeur propre λ. L'ensemble des valeurs propre est appelé spectre de u, noté* $\mathrm{Sp}(u)$

Proposition 3.1.2. *Soit $u \in \mathscr{L}(E)$, et $\lambda \in \mathbb{K}$. Sont équivalents :*

(i) *λ est valeur propre de u.*

(ii) *λ est racine de χ_u.*

(iii) *λ est racine de π_u.*

3.2 Réduction des endomorphismes

3.2.1 Diagonalisation

Définition 3.2.1 (Endomorphisme diagonalisable)**.** *Soit $u \in \mathscr{L}(E)$. On dit que u est diagonalisable s'il existe une base $\mathcal{B}$ de E telle que $\mathrm{mat}_{\mathcal{B}}(u)$ soit diagonale.*

Théorème 3.2.1. *Soit $u \in \mathscr{L}(E)$. Sont équivalents :*

(i) *u est diagonalisable.*

(ii) $E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u)$.

(iii) $\dim E = \sum_{\lambda \in \mathrm{Sp}(u)} \dim E_\lambda(u)$.

(iv) *Il existe un polynôme annulateur de u scindé à racines simples.*

(v) *π_u est scindé à racines simples.*

(vi) *$\chi_u = \prod_{\lambda \in \mathbb{K}} (X - \lambda)^{m_\lambda}$ avec pour tous $\lambda \in \mathrm{Sp}(u)$, $m_\lambda = \dim E_\lambda(u)$.*

3.2.2 Réduction de Jordan

Définition 3.2.2. *Soit $u \in \mathscr{L}(E)$. L'endomorphisme u est dit nilpotent s'il existe $r \in \mathbb{N}^*$ tel que $u^r = 0_{\mathscr{L}(E)}$. On appelle indice de nilpotence de u le plus petit r entier vérifiant cette propriété.*

Remarque. La famille $(x, u(x), \dots, u^{r-1}(x))$ est libre, donc $r \leq \dim(E)$.

Définition 3.2.3. *Soit $n \in \mathbb{N}^*$. On appelle bloc de* Jordan *nilpotent de taille n la matrice :*

$$J_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$$

Théorème 3.2.2. *Soit E un $\mathbb{K}$-e.v de dimension finie, et $u \in \mathscr{L}(E)$ un endomorphisme nilpotent. Il existe une unique famille d'entiers $(n_1, \dots, n_r)$ avec $n_1 \geq n_2 \geq \dots \geq n_r > 0$ et $\mathcal{B}$ une base de E, tels que :*

$$\mathrm{mat}_{\mathcal{B}}(u) = \begin{pmatrix} J_{n_1} & (0) & \dots & (0) \\ (0) & J_{n_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & (0) \\ (0) & \cdots & (0) & J_{n_r} \end{pmatrix}$$

Remarques.

- On remarque que la matrice a exactement r colonnes nulles, donc r est en fait la dimension du noyau de u.
- Si $n \geq 2$, alors $\dim\ker(J_n^2) = 2$, et $\dim\ker(J_1^2) = 1$. Ainsi :

$$\dim\ker(u^2) = 2 \cdot \mathrm{card}\left(\{i \in [\![1, r]\!] \,|\, n_i \geq 2\}\right) + \mathrm{card}\left(\{i \in [\![1, r]\!] \,|\, n_i = 1\}\right)$$

Et :

$$\dim\ker(u^2) - \dim\ker(u) = \mathrm{card}\left(\{i \in [\![1, r]\!] \,|\, n_i \geq 2\}\right)$$

Ce qui se généralise pour $j \in \mathbb{N}^*$:

$$\dim\ker(u^j) - \dim\ker(u^{j-1}) = \mathrm{card}\left(\{i \in [\![1, r]\!] \,|\, n_i \geq j\}\right)$$

Démonstration. Montrons le résultat par récurrence sur $n = \dim E$. Pour $n = 0$, c'est clair. Soit désormais $n \in \mathbb{N}^*$, et supposons le résultat acquis pour tout espace de dimension inférieure à n. Notons s l'indice de nilpotence de u. Si $s = n$, le résultat est démontré puisque la remarque sur les endomorphismes nilpotents nous fournit une base adaptée, et s ne dépend pas du choix de la base. Soit $F = \mathrm{Vect}(x, u(x), \dots, u^{r-1}(x)) \subsetneq E$. Soit $\phi \in E^*$ une forme linéaire telle que $\phi(u^{s-1}(x)) = 1$ et

$\phi(u^i(x)) = 0$ pour tous $0 \leq i < s-1$. On note alors $\Gamma = \mathrm{Vect}({}^t u^i(\phi))_{i\in\mathbb{N}}$, et $G = \Gamma^{\perp}$. Ainsi construit, Γ est stable par ${}^t u$, et donc G est stable par u. Montrons maintenant que $E = F \oplus G$:

— Soit $y = \sum_{i=0}^{s-1} \lambda_i u^i(x) \in G$, alors ${}^t u^{s-1}(\phi)(y) = 0$, donc en itérant, on trouve λ_0. Par récurrence, on trouve que $y = 0$.

— Pour terminer, on vérifie que $\dim F = \dim \Gamma$. En effet, ${}^t u$ est nilpotente d'indice s, donc $(\phi, \ldots, {}^t u(\phi))$ est une base de Γ

On applique alors l'hypothèse de récurrence à G, puisque l'endomorphisme induit par u sur G est nilpotent d'indice inférieur à s. Pour l'unicité des n_i, on utilise le fait que

□

Définition 3.2.4. *Soient $\lambda \in \mathbb{K}$, $n \in \mathbb{N}^*$. On appelle bloc de* Jordan *de taille n la matrice $J_{\lambda,n} = \lambda I_n + J_n$.*

Théorème 3.2.3 (Décomposition de Jordan)**.** *Soit E un $\mathbb{K}$-e.v de dimension finie, et $u \in \mathscr{L}(E)$. On suppose χ_u scindé. Alors, il existe une base de E dans laquelle la matrice de u est diagonale par blocs, les blocs étant de la forme $J_{\lambda,j}$. De plus, les blocs qui apparaissent ne dépendent pas de la base choisie.*

Démonstration. Notons $\chi_u = \prod_{\lambda\in\mathrm{Sp}(u)} (X-\lambda)^{n_\lambda}$. Pour tous λ est valeur propre de u, on note l'espace caractéristique associé $F_\lambda = \ker(u - \lambda\,\mathrm{id}_E)^{n_\lambda}$. Le lemme des noyaux assure la décomposition :

$$E = \bigoplus_{\lambda\in\mathrm{Sp}(u)} F_\lambda$$

Pour toute valeur propre λ de u, on note u_λ l'endomorphisme induit par u sur F_λ. On applique alors le résultat précédent à tous les endomorphismes u_λ, et on concatène les bases obtenues. Pour l'indépendance quant au choix de la base, on remarque la diagonale sera composée des valeurs propres. Enfin, l'unicité des blocs est donnée par le théorème précédent.

□

3.2.3 Endomorphismes cycliques et réduction de Frobenius

Endomorphismes cycliques

Définition 3.2.5. *Soit E un $\mathbb{K}$-e.v.Un endomorphisme $u \in \mathscr{L}(E)$ s'il existe $x \in E$ tel que* $\mathrm{Vect}(u^i(x))_{i\in\mathbb{N}} = E$*. Un tel x est dit vecteur cyclique de u.*

Remarque. Pour $x \in E$ un vecteur quelconque, $\mathrm{Vect}(u^i(x))_{i\in\mathbb{N}}$ est le plus petit sous-espace stable par u contenant x.

Proposition 3.2.1. *On suppose E de dimension finie. Soit $u \in \mathscr{L}(E)$, u est cyclique si et seulement si il existe $n \in \mathbb{N}^*$ tel que $(x, u(x), \ldots, u^{n-1}(x))$ soit une base de E.*

Démonstration. Soit $x \in E$ vecteur cyclique de u et $n = \dim E$. Soit $i \geq n$, on effectue la division euclidienne de X^i par χ_u. Alors on trouve $u^i = R(u)$ avec R un polynôme de degré inférieur à n (qui est le degré de χ_u). On en déduit que $u^i(x) \in \mathrm{Vect}(x, u(x), \ldots, u^{n-1}(x))$. Le sens réciproque est clair.

□

Définition 3.2.6 (Matrice compagnon)**.** *Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}[X]$. On appelle matrice compagnon associée à P la matrice*

$$\mathcal{C}_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Proposition 3.2.2. *Soit $P \in \mathbb{K}[X]$ un polynôme unitaire.*

$$\chi_{\mathcal{C}_P} = P$$

Théorème 3.2.4 (Réduction de FROBENIUS)**.** *Soit $u \in \mathscr{L}(E)$. Alors il existe une unique famille de polynômes unitaires $(P_1, \ldots, P_r)$, une famille $(E_1, \ldots, E_r)$ de sous-espaces stables par u, tels que :*

(i) $E = \bigoplus_{1 \leq i \leq r} E_i$.

(ii) *Pour tous $i \in [\![1, r]\!]$, l'endomorphisme induit par u sur E_i est cyclique de polynôme P_i.*

(iii) $P_r | P_{r-1} | \cdots | P_1$.

Les P_i sont appelés les ***invariants de similitudes*** *de P.*

Remarques.

— u est cyclique *si et seulement si* dans une certaine base $\mathcal{B}$, sa matrice est une matrice compagnon.

— Si u est cyclique, $\chi_u = \pi_u$. En effet, si x est vecteur cyclique de u et P est un polynôme de degré strictement inférieur à n, alors $P(u)(x) = 0$ impose que $P = 0$ puisque $(x, u(x), \ldots, u^{n-1}(x))$ est une famille libre. Donc le polynôme annulateur de u est nécessairement de degré égal à celui du polynôme caractéristique.

— Si x est vecteur cyclique de u, $\{P \in \mathbb{K}[X] \,|\, P(u)(x) = 0\}$ est un idéal non nul de $\mathbb{K}[X]$. Soit $\pi_{u,x}$ son unique générateur unitaire. Alors pour tous $x \in E$, $\pi_{u,x} | \pi_u$. De plus, il existe un $x_0 \in E$ tel que $\pi_{u,x_0} = \pi_u$. On peut par exemple démontrer ce résultat lorsque $\mathbb{K}$ est infini. L'ensemble $\{\ker(\pi_{u,x}(u)) \,|\, x \in E\}$ est fini car π_u n'a qu'un nombre fini de diviseurs unitaires. Cependant,

$$E = \bigcup_{x \in E} \ker(\pi_{u,x}(u))$$

est une union finie d'espaces vectoriels. On sait alors qu'il existe un x_0 tel que $E = \ker \pi_{u,x_0}(u)$, car le corps de base est infini.

Démonstration. Soit $x_0 \in E$ tel que $\pi_{u,x_0} = \pi_u$, et l'on pose $F = \mathrm{Vect}(u^i(x_0)_{i\in\mathbb{N}})$. Une base de F est $(x_0, u(x_0), \dots, \dots, u^{d-1}(x_0))$, où d est le degré de π_u. Soit $\varphi \in E^*$, une forme linéaire telle que $\varphi(x_0) = \varphi(u(x_0)) = \cdots = \varphi(u^{d-2}(x_0)) = 0$, et $\varphi(u^{d-1}(x_0)) = 1$. Posons $\Gamma = \mathrm{Vect}({}^t u^i(\varphi))_{i\in\mathbb{N}}$. Montrons maintenant que $E = F \oplus \Gamma^\circ$, et que Γ° est stable par u.

— Γ° est stable par u car Γ l'est par ${}^t u$.

— Soit $P \in \mathbb{K}[X]$. On a $P({}^t u)(\varphi) = \varphi \circ P(u)$. Si $P(u) = 0$, alors $P({}^t u)(\varphi) = 0$, donc $\pi_{{}^t u,\varphi} | \pi_u$. Soit maintenant $P = \sum_{k=0}^{d-1} X^k \in \mathbb{K}[X]$ tel que $P({}^t u)(\varphi) = 0_{E^*}$. On a alors $0_{\mathbb{K}} = P({}^t u)(\varphi)(x_0) = \varphi\left(\sum_{k=0}^{d-1} u^k(x_0)\right) = a_{d-1}$. En évaluant successivement en $u(x_0), u^2(x_0), \dots$, on trouve que $P = 0$. Cela montre que tout polynôme P de degré inférieur au degré de π_u vérifiant $P({}^t u)(\varphi) = 0$ est nécessairement nul. On en déduit donc que $\pi_{{}^t u,\varphi} = \pi_u$. Cela nous indique en particulier que $\dim \Gamma = \deg \pi_{{}^t u,\varphi} = d$.

— On montre de la même façon que $F \cap \Gamma^\circ = \{0_E\}$.

Par récurrence sur la dimension de E, on montre que la décomposition existe. Si $\dim E = 0$, c'est clair. Soit $n \in \mathbb{N}^*$. On suppose le résultat acquis pour tous espaces de dimensions inférieurs strictement à n, et on reprend les notations du début de démonstration. Si $\dim F = \dim E$, alors u est cyclique, et $P_1 = \chi_u = \pi_u$. Dans le cas où $\dim F < \dim E$, on a aussi $\dim \Gamma^\circ < E$. On applique alors l'hypothèse de récurrence à $(\Gamma^\circ, u_{\Gamma^\circ})$. On a alors $\Gamma^\circ = \bigoplus_{i=2}^r E_i$ avec u_{E_i} cyclique de polynôme minimal P_i, avec $P_r | P_{r-1} | \cdots | P_2$. On pose de plus $P_1 = \pi_{u_F} = \pi_u$. Pour tous $y \in \Gamma^\circ$, on a $\pi_u(u)(y) = 0$, donc $\pi_{u_{E_i}} | \pi_u$ pour tous $i \in [\![2, r]\!]$.

Montrons désormais l'unicité [1]. On suppose $E = \bigoplus_{i=1}^r E_i = \bigoplus_{j=1}^s F_j$, des décompositions de FROBENIUS associées à des invariants de similitudes respectifs $(P_1, \dots, P_r)$ et $(Q_1, \dots, Q_s)$. D'une part, on a $P_1 = Q_1 = \pi_u$. Soit $k \in \mathbb{N}$ le plus petit entier tel que $P_k \neq Q_k$. On a

$$P_k(u)(E) = \bigoplus_{i=1}^{k-1} P_k(u)(E_i)$$

et

$$P_k(u)(E) = \bigoplus_{i=1}^{s} P_k(u)(F_i).$$

Or, pour tout $i \in [\![1, k-1]\!]j$, $P_i(u)(E_i) = Q_i(u)(F_i) = P_i(u)(F_i)$ par hypothèse. On observe donc que pour tout $j \in [\![k, j]\!]$, $\dim P_k(u)(F_j) = 0$. Ainsi, Q_k divise P_k. Symétriquement, on montre aussi que Q_k divise P_k et donc que $P_k = Q_k$, ce qui contredit l'existence de k. D'où l'unicité. $\square$

Exemples.

— Si $u \in \mathscr{L}(E)$ est cyclique, il admet un seul invariant de similitude (χ_u).

— Si $u = 0$, la famille de ses invariants de similitudes est $(X, \dots, X)$ (autant de fois que la dimension).

— Si $u \in \mathscr{L}(E)$ est nilpotent de blocs de JORDAN de tailles $m_1 \geq \cdots \geq m_r$, alors ses invariants de similitude sont $(X^{m_1}, \dots, X^{m_r})$.

1. Moi aussi j'en peux plus.

Corollaire 3.2.1. *Soit E un $\mathbb{K}$-e.v de dimension finie.*

(i) Soient $u, v \in \mathscr{L}(E)$. u et v sont semblables si et seulement si ils ont les mêmes invariants de similitudes

(ii) Soit $u \in \mathscr{L}(E)$. Si χ_u est scindé à racines simples, alors u est cyclique.

(iii) Les invariants de similitudes (et en particulier le polynôme minimal) ne dépendent pas du corps.

Proposition 3.2.3. *Soit $u \in \mathscr{L}(E)$. Si χ_u est scindé, alors il existe un couple $(d, n) \in \mathscr{L}(E)^2$ tel que d est diagonalisable, d est nilpotente, $u = d + n$, et d et n commutent. De plus, d et n sont des polynômes en u et sont uniques.*

Chapitre 4

Espaces quadratiques

4.1 Formes quadratiques et formes bilinéaires

4.1.1 Définitions

Dans cette section, $\mathbb{K}$ désignera un corps de caractéristique différente de 2, et E sera un $\mathbb{K}$-espace vectoriel.

Définition 4.1.1. *Soit $q : E \longrightarrow \mathbb{K}$. On dit que q est une forme quadratique sur E si :*

- $\forall x \in E$, $\forall \lambda \in \mathbb{K}$, $q(\lambda x) = \lambda^2 q(x)$
- *L'application $(x, y) \longmapsto q(x + y) - q(x) - q(y)$ est une forme bilinéaire symétrique sur $E \times E$.*

Remarque et exemple.

— On appelle *espace quadratique* la donnée (E, q) d'un $\mathbb{K}$-espace vectoriel et d'une forme quadratique q.

— Sur $\mathbb{K}^n$, l'application $(x_1, \ldots, x_n) \longmapsto \sum_{i=1}^n x_i^2$ est une forme quadratique.

Définition 4.1.2. *Soit $q : E \longrightarrow \mathbb{K}$ une forme quadratique. On appelle forme polaire de q la forme bilinéaire $(x, y) \longmapsto \dfrac{1}{2}[q(x + y) - q(x) - q(y)]$.*

La forme polaire de q est l'unique forme bilinéaire symétrique b sur $E \times E$ telle que :

$$\forall x \in E,\ q(x) = b(x, x)$$

En effet, on vérifie facilement que b vérifie la relation. Elle est unique car elle est entièrement déterminée par q.

Définition 4.1.3. *Soient (E, q) et (F, r) deux $\mathbb{K}$-e.v munis d'une forme quadratique (espaces quadratiques). On appelle morphisme métrique de E vers F toute application $u \in \mathscr{L}(E, F)$ telle que $q = r \circ u$. On dit que E et F sont isométriques s'il existe un isomorphisme de E dans F qui soit métrique. Un tel isomorphisme est appelé isométrie.*

Remarque. Puisqu'une isométrie est un isomorphisme, u^{-1} est aussi une isométrie. La qualité d'isométrie entre deux espaces définit en fait une relation d'équivalence. Cette notion est majeure, car ce cours s'intéressera à la classification des espaces quadratiques à isométrie près.

Proposition 4.1.1. *Une application $q : E \longrightarrow \mathbb{K}$ est une forme quadratique si et seulement si son écriture en coordonnées est un polynôme homogène de degré 2 en les coordonnées.*

Démonstration. Soit $(e_1, \ldots, e_n)$ une base de E. Supposons que q est une forme quadratique. Notons b sa forme polaire. Soit $x = \sum_{i=1}^{n} x_i e_i$, on a :

$$\begin{aligned} q(x) &= b(x,x) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j b(e_i, e_j) \end{aligned}$$

Réciproquement, si $q(x) = \sum_{i,j=1}^{n} \lambda_{i,j} x_i x_j$, on a clairement que $q(\lambda x) = \lambda^2 q(x)$ pour tout $\lambda \in \mathbb{K}$.

Notons $B(x,y) = q(x+y) - q(x) - q(y)$ pour $x, y \in E$, B est clairement symétrique. Soient $x, y, z \in E$, et $\lambda \in \mathbb{K}$.

$$B(x, y+\lambda z) - B(x,y) - \lambda B(x,z)$$
$$= q(x + (y+\lambda z)) - q(x) - q(y+\lambda z) - (q(x+y) - q(x) - q(y)) - \lambda(q(x+z) - q(x) - q(z))$$

En développant avec l'expression polynômiale de q, on trouve 0.[1]

□

4.1.2 Noyau d'une forme quadratique

Définition 4.1.4. *Soit (E,q) un espace quadratique, et b la forme polaire de q. On appelle noyau de q l'ensemble :*

$$\left\{x \in E \,|\, \forall y \in E,\, b(x,y) = 0\right\}$$

On dit que q est dégénérée si ce noyau n'est pas réduit à 0, et non dégénérée sinon.

Remarque. $N(q) \subset I(q) = \{x \in E \,|\, q(x) = 0\}$.

Théorème 4.1.1 (Représentation)**.** *Soit (E,q) un espace quadratique, et b la forme polaire de q. Sont équivalents :*

(i) q est non dégénérée.

(ii) L'application linéaire :

$$\varphi_q : \begin{array}{ccc} E & \longrightarrow & E^* \\ x & \longmapsto & f_x : \left| \begin{array}{ccc} E & \longrightarrow & \mathbb{K} \\ y & \longmapsto & b(x,y) \end{array} \right. \end{array}$$

est un isomorphisme.

1. Non mais franchement, je vais pas écrire ça.

Remarque. $N(q) = \ker(\varphi_q)$.

4.1.3 Représentation matricielle

Définition 4.1.5. *Soit (E, q) un espace quadratique sur le corps $\mathbb{K}$, de forme polaire b. Soit $\mathcal{B}$ une base de E. On appelle matrice de q dans la base $\mathcal{B}$ la matrice de φ_q dans les bases $\mathcal{B}$ et $\mathcal{B}^*$.*

Remarque. Si $\mathcal{B} = (e_1, \dots, e_n)$, la matrice de q est aussi la matrice $(b(e_i, e_j))_{i,j}$. En effet, si on note $M = (m_{i,j})_{i,j}$ cette matrice, alors si $i, j \in [\![1, n]\!]$,

$$\varphi_q(e_i) = \sum_{k=1}^{n} m_{i,k} e_k^*.$$

Ainsi,

$$b(e_i, e_j) = \varphi_q(e_i)(e_j) = \sum_{k=1}^{n} m_{i,k} e_k^*(e_j).$$

D'où $m_{i,j} = b(e_i, e_j)$.

Proposition 4.1.2. *Soit (E, q) un espace quadratique et M la matrice de q dans la base $\mathcal{B} = (e_1, \dots, e_n)$. Soit $x \in E$, de vecteur dans la base $\mathcal{B}$, X. En identifiant $\mathbb{K}$ à $\mathcal{M}_1(\mathbb{K})$, on a $q(x) = {}^t XMX$. Si $u \in \mathrm{GL}(E)$ et P est la matrice de u dans la base précédente, alors la matrice de q dans la base $(u(e_1), \dots, u(e_n))$ est ${}^tPMP$.*

Remarque. On définit alors le rang de la forme quadratique q comme le rang de la matrice de q dans une quelconque base de E. C'est exactement le rang de φ_q.

Proposition 4.1.3. *Soient $(E, q), (F, r)$ deux espaces quadratiques de dimension finie n. Sont équivalents :*

(i) Les espaces quadratiques E et F sont isométriques.

(ii) Il existe une base $\mathcal{B}_E$ de E et une base $\mathcal{B}_F$ de F, dans lesquelles q et r ont même matrice.

(iii) Pour toutes bases $\mathcal{B}_E$ de E et $\mathcal{B}_F$ de F, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que :

$${}^tP \,\mathrm{mat}_{\mathcal{B}_E}(q) P = \mathrm{mat}_{\mathcal{B}_F}(r).$$

Définition 4.1.6. *On note $\mathbb{K}/(\mathbb{K}^\times)^2$ l'espace quotient $\mathbb{K}/\!\sim$ où $\sim$ est une relation d'équivalence définie par :*

$$\forall x, y \in \mathbb{K},\ (x \sim y) \iff (\exists z \in \mathbb{K}^\times,\ x = z^2 y)$$

Définition 4.1.7 (Discriminant)**.** *Soit (E, q) un espace quadratique de dimension finie, et M la matrice de q dans une base de E. On appelle discriminant de q l'image de $\det(M)$ dans $\mathbb{K}/(\mathbb{K}^\times)^2$. On note $\operatorname{disc}(M)$ le discriminant de q.*

Proposition 4.1.4. *(i) Si deux espaces quadratiques (E, q) et (F, r) sont isométriques, alors $\operatorname{disc}(q) = \operatorname{disc}(r)$.*

(ii) Soit (E, q) un espace quadratique. q est non dégénérée si et seulement si son discriminant est non nul.

4.2 Orthogonalité

4.2.1 Définition

Définition 4.2.1. *Soit (E, q) un espace quadratique, et b la forme polaire de q. Soit $A \subset E$. On appelle orthogonal de A l'ensemble :*

$$A^\perp = \{y \in E \,|\, \forall x \in A,\, b(x, y) = 0\}$$

On dit que B est orthogonal à A si $B \subset A^\perp$. Un somme directe $\bigoplus_{i=1}^r E_i$ est dit orthogonale si pour tous $i, j \in [\![1, r]\!]$, si $i \neq j$, alors E_i est orthogonal à E_j.

Remarques.

— Si une somme directe est orthogonale, on note parfois pour une somme de deux espaces :

$$E_1 \overset{\perp}{\oplus} E_2$$

— On a $N(q) = E^\perp$, et $I(q) = \big\{x \in E \,|\, x \in \{x\}^\perp\big\}$.

— Soit F un supplémentaire de $N(q)$, alors $E = F \overset{\perp}{\oplus} N(q)$, et $q_{|F}$ est non dégénérée.

Proposition 4.2.1. *Soit (E, q) un espace quadratique non dégénéré de dimension finie, et soit F un s.e.v de E. Alors $F^\perp = \varphi_q^{-1}(F^\circ)$. En particulier :*

$$\dim E = \dim F + \dim F^\perp$$

Remarque. On n'a pas nécessairement $E = F \oplus F^\perp$. La proposition suivante donne une condition nécessaire et suffisante pour réaliser la supplémentarité.

Proposition 4.2.2. *Sous les mêmes hypothèses, $E = F \oplus F^\perp$ si et seulement si $F \cap F^\perp = \{0_E\}$ (i.e si $q_{|F}$ est non dégénérée).*

4.2.2 Classification des espaces quadratiques sur $\mathbb{R}$ et $\mathbb{C}$

Théorème 4.2.1. *Soit (E, q) un espace quadratique de dimension finie n. Soit $\mathcal{F}$ une famille de représentants de $\mathbb{K}^\times/(\mathbb{K}^\times)^2$. Il existe une base de E constituée d'éléments e_i deux à deux orthogonaux, tels que $q(e_i) \in \mathcal{F} \cup 0$ pour tout $i \in [\![1, n]\!]$.*

Proposition 4.2.3 (Réduction de Gauss)**.** *Il existe un algorithme permettant d'écrire une forme quadratique en coordonnées sous la forme*

$$q(x_1, \dots, x_n) = \sum_{i=1}^{r} a_i f_i(x_1, \dots, x_n)^2$$

où les f_i sont des formes linéaires indépendantes, et $a_i \in \mathbb{K}$ pour tout indice i.

Théorème 4.2.2. *Soit (E, q) un espace quadratique sur $\mathbb{C}$, non dégénéré de dimension finie. Il existe une base de E dans laquelle la matrice de q est l'identité.*

Démonstration. Soit n la dimension de E. Remarquons avant tout que $\mathbb{C}/(\mathbb{C})^2$ ne possède que deux éléments (la classe de 0 et de 1). Le théorème précédent assure l'existence d'une base $(e_1, \dots, e_n)$ d'éléments deux à deux orthogonaux et tels que $q(e_i) = 1$ pour tout indice i (q étant non dégénérée, $q(e_i)$ est nécessairement non nul). On a alors pour tout $i, j \in [\![1, n]\!]$,

$$b(e_i, e_j) = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon.} \end{cases}$$

$\square$

Corollaire 4.2.1. *Soient (E, q) et (F, r) deux espaces quadratiques sur C. E et F sont isométriques si et seulement si ils sont de même dimension, et q et r sont de même rang.*

Théorème 4.2.3 (d'inertie de Sylvester)**.** *Soit (E, q) un espace quadratique de dimension finie sur $\mathbb{R}$. Alors il existe une base de E dans laquelle la matrice de q est de la forme :*

$$\begin{pmatrix} I_s & (0) & (0) \\ (0) & -I_t & (0) \\ (0) & (0) & (0) \end{pmatrix}$$

De plus, les entiers s et t ne dépendent pas du choix de la base.

Démonstration. Une famille de représentants de $\mathbb{R}^*/(\mathbb{R}^*)^2$ est $\{\pm 1\}$.

$\square$

Définition 4.2.2. *Le couple (s, t) est appelé signature de q.*

Remarques.

— $s+t$ est le rang de q.

— On peut calculer le couple (s,t) avec l'algorithme de réduction de Gauss. Par exemple, si on définit une forme quadratique q sur $\mathbb{R}^3$ par $q(x,y,z) = y^2 - z^2 + 2(xy+yz)$, la signature de q est $(1,2)$.

— Une forme quadratique réelle non dégénérée admet un vecteur isotrope non nul *si et seulement si* sa signature n'est pas de la forme $(n,0)$ ou $(0,n)$. En reprenant l'exemple précédent, cela signifie que l'équation $q(x,y,z)=0$ admet une solution non nulle.

4.2.3 Groupe orthogonal d'une forme quadratique

Définition 4.2.3. *Soit (E,q) un espace quadratique. On appelle groupe orthogonal le groupe $\mathcal{O}(q)$ des isométries de E.*

Notation. Soit $x \in E$ un vecteur non isotrope. On appelle réflexion d'axe x l'application :

$$\sigma_x : \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & y - 2\frac{b(x,y)}{q(x)}x \end{array}$$

C'est une isométrie.

Théorème 4.2.4. *Soit (E,q) un espace quadratique. Si (E,q) est non dégénérée, alors $\mathcal{O}(q)$ est engendrée par les réflexions.*

4.3 Adjoints et endomorphismes normaux

4.3.1 Adjoint d'un endomorphisme

Proposition 4.3.1. *Soient (E,q) et (F,r) des espaces quadratiques de formes polaires respectives b_E et b_F. On suppose (E,q) non dégénéré de dimension finie. Soit $u \in \mathscr{L}(E,F)$. Alors, il existe un unique $u^* \in \mathscr{L}(F,E)$ tel que :*

$$\forall (x,y) \in E \times F,\, b_F(u(x),y) = b_E(x,u^*(y))$$

*u^* est appelé **adjoint** de u.*

Proposition 4.3.2. *Sous les mêmes hypothèses et en supposant les espaces tous deux non dégénérés de dimensions finies, alors :*

$$\begin{array}{ccc} \mathscr{L}(E,F) & \longrightarrow & \mathscr{L}(F,E) \\ u & \longmapsto & u^* \end{array}$$

est un isomorphisme. De plus, pour tout $u \in \mathscr{L}(E,F)$, $(u^*)^* = u$.

Proposition 4.3.3. *Soit (E, q) un espace quadratique non dégénéré de dimension finie. Alors :*

$$\forall u, v \in \mathscr{L}(E),\ (uv)^* = v^* u^*$$

Démonstration. On note b la forme polaire de q. Soient $x, y \in E$. On a

$$b(u(v(x)), y) = b(v(x), u^*(x)) = b(x, v^*(u^*(y))).$$

Par unicité de l'adjoint, $(uv)^* = v^* u^*$.

□

Proposition 4.3.4. *Soit (E, q) un espace quadratique de dimension finie, non dégénéré. Soit $u \in \mathscr{L}(E)$, et soit F un sous-espace stable par u. Alors $F^\perp$ est stable par u^*.*

Démonstration. Soit $x \in F^\perp$. Alors pour tout $y \in F$, $b(u^*(x), y) = b(x, u(y)) = 0$ car $u(y) \in F$.

□

4.3.2 Endomorphisme normal

Définition 4.3.1. *Un endomorphisme $u \in \mathscr{L}(E)$ est dit normal s'il commute avec son adjoint.*

Proposition 4.3.5. *Soit (E, q) un espace quadratique non dégénéré de dimension finie. Soit $u \in \mathscr{L}(E)$ un endomorphisme normal. Alors pour tout $P \in \mathbb{K}[X]$, $\ker P(u)$ est stable par u^*.*

Chapitre 5

Espaces euclidiens et hermitiens

5.1 Formes hermitiennes

5.1.1 Applications remarquables sur des $\mathbb{C}$-e.v

Définition 5.1.1 (Semi-linéarité). *Soit E et F des $\mathbb{C}$-e.v, et $f : E \longrightarrow F$. f est dite semi-linéaire si*

$$\forall x, y \in E, \forall \lambda \in \mathbb{C}, \ f(x + \lambda y) = f(x) + \overline{\lambda} f(y).$$

Définition 5.1.2 (Sesquilinéarité). *Soit E un $\mathbb{C}$-e.v. Une forme sesquilinéaire sur E est une application $f : E \times E \longrightarrow \mathbb{C}$ telle que :*

— *Pour tout $y \in E$, $f(\,\cdot\,, y)$ est linéaire.*

— *Pour tout $x \in E$, $f(x, \,\cdot\,)$ est semi-linéaire.*

Définition 5.1.3 (Forme hermitienne). *Soit E un $\mathbb{C}$-e.v. Une forme hermitienne sur E est une forme sesquilinéaire telle que*

$$\forall x, y \in E, \ f(x, y) = \overline{f(y, x)}.$$

5.1.2 Produit scalaire et espace associé

Définition 5.1.4. *Soit E un $\mathbb{C}$-e.v (resp. $\mathbb{R}$-e.v). Un produit scalaire sur E est la donnée d'une forme hermitienne (resp. bilinéaire symétrique) f telle que :*

— $\forall x \in E, \ f(x, x) \geq 0.$

— $\forall x \in E, \ f(x, x) = 0 \iff x = 0_E.$

C'est-à-dire que f est définie positive.

Définition 5.1.5. *Un espace hermitien (resp. euclidien) est un espace vectoriel de dimension finie sur $\mathbb{C}$ (resp. sur $\mathbb{R}$) muni d'un produit scalaire.*

Exemples.

— $(\mathbb{R}^n, \langle \cdot \mid \cdot \rangle)$ où $\langle x|y \rangle = \sum_{i=1}^n x_i y_i$ est un espace euclidien.

— $(\mathbb{C}^n, \langle \cdot \mid \cdot \rangle)$ où $\langle x|y \rangle = \sum_{i=1}^n x_i \overline{y_i}$ est un espace hermitien.

— $(\mathbb{C}_n[X], \langle \cdot \mid \cdot \rangle)$ où

$$\langle P|Q \rangle = \int_0^1 P(t)\overline{Q(t)}\mathrm{d}t$$

est un espace hermitien.

Définition 5.1.6. *Soit $(E, \langle \cdot \mid \cdot \rangle)$ un espace hermitien ou euclidien, et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. On appelle matrice du produit scalaire dans la base $\mathcal{B}$ la matrice $\big(\langle e_i|e_j \rangle\big)_{i,j \in [\![1,n]\!]}$.*

Remarque. Ainsi définie, on a pour tout $x, y \in E$, $\langle x|y \rangle = {}^tXM\overline{Y}$.

5.1.3 Inégalité de Cauchy-Schwartz

Proposition 5.1.1 (Inégalité de Cauchy-Schwartz)**.** *Soit $(E, \langle \cdot \mid \cdot \rangle)$ un espace euclidien ou hermitien. Alors :*

$$\forall x, y \in E, \ \big|\langle x \mid y \rangle\big|^2 \leq \langle x \mid x \rangle \langle y \mid y \rangle$$

Remarque. L'inégalité de Cauchy-Schwartz est loin d'être sans conséquence, et apparaît même souvent en analyse. Par exemple, elle permet de démontrer que la fonction Γ d'Euler est convexe.

Corollaire 5.1.1. *Soit $(E, \langle \cdot \mid \cdot \rangle)$ un espace euclidien ou hermitien. L'application :*

$$\begin{array}{rccc} \|\cdot\|_2 : & E & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \sqrt{\langle x \mid x \rangle} \end{array}$$

est une norme sur E.

5.2 Réduction des normaux, décomposition polaire

Lemme 5.2.1. *Soit $u \in \mathscr{L}(E)$, et F stable par u. Alors, $F^\perp$ est stable par u^*. En outre, si u est normal, et si $F = \ker P(u)$ pour un quelconque $P \in \mathbb{K}[X]$, alors $F^\perp$ est stable par u.*

Démonstration. Si F est stable par u, alors $F^\perp$ est stable par u^* (déjà vu). Supposons u normal, et $F = \ker P(u)$ (avec $P \in \mathbb{K}[X]$ quelconque). F est stable par tout endomorphisme commutant avec u, donc F est en particulier stable par u^*. Donc F est stable par $(u^*)^* = u$. Sous ces conditions, on a $E = F \oplus F^\perp$ en somme orthogonale.

□

Théorème 5.2.1. *Soit E un espace hermitien. Un endomorphisme $u \in \mathscr{L}(E)$ est normal si et seulement si il est diagonalisable en base orthonormée.*

Démonstration. Démontrons ce théorème par récurrence sur $n = \dim E$.

- $n = 0$. Évident.
- Soit $n > 0$. On suppose le résultat vrai sur tout espace de dimension $k < n$. Soit $\lambda \in \mathbb{C}$ valeur propre [1] de u. Soit $F = E_\lambda(u) = \ker(u - \lambda \operatorname{id}_E)$. F et $F^\perp$ sont stables par u et u^*, et $E = F \oplus F^\perp$ (somme directe orthogonale). Or, $u_{F^\perp}$ est normal, et par hypothèse de récurrence, il existe une base orthonormée de $F^\perp$ constituée de vecteurs propres de u. De plus, $u_F = \lambda \operatorname{id}_F$, donc toute base de F est constituée de vecteurs propres de u.

$\square$

Lemme 5.2.2. *Soit E un espace euclidien de dimension 2, et soit $u \in \mathscr{L}(E)$. On suppose u normal, et sans valeur propre réelle. Alors dans toute base orthonormée, la matrice de u est de la forme :*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

*On appelle une telle matrice une **matrice de similitude**.*

Démonstration. **Rappel.** Si $\mathcal{B}$ est une base orthonormée, et $u \in \mathscr{L}(E)$, alors $\operatorname{mat}_{\mathcal{B}}(u) = {}^t\operatorname{mat}_{\mathcal{B}}(u^*)$. Soit $\mathcal{B}$ une base orthonormée de E, $u \in \mathscr{L}(E)$ un endormorphisme, et l'on note :

$$M = \operatorname{mat}_{\mathcal{B}}(u) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

On a alors $\chi_u = X^2 - (a+d)X + (ad - bc)$, et son discriminant est $\Delta_u = (a-d)^2 + 4bc < 0$ (car u n'a aucune valeur propre réelle). On calcule ensuite ${}^tMM$ et $M{}^tM$ (donc les produits de la matrice de u et celle de u^*). On trouve alors que u est normal *si et seulement si* $a = d$ et $b = -c$.

$\square$

Théorème 5.2.2. *Soit E un espace euclidien, et $u \in \mathscr{L}(E)$ un endomorphisme normal. Alors, il existe une base orthonormée dans laquelle la matrice de u est diagonale par blocs, les blocs étant de taille 1, ou de taille 2 (et sont des matrices de similitudes).*

Remarque. On sait déjà que qu'un endomorphisme normal sur un espace hermitien est diagonalisable en base orthonormée. Mais on sait aussi que si $\lambda \in \mathbb{C} \backslash \mathbb{R}$, alors :

$$\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \text{ est semblable (dans } \mathcal{M}_n(\mathbb{C})\text{) à } \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix}$$

Où $\lambda = |\lambda| e^{i\theta}$.

1. Il y a toujours une valeur propre car $\mathbb{C}$ est algébriquement clos.

Démonstration. On démontre le théorème par récurrence sur $n = \dim E$. Si u a une valeur propre réelle, la démonstration est la même que sur $\mathbb{C}$. Sinon, on se ramène au cas où u n'a pas de valeur propre réelle : soit $P \in \mathbb{R}[X]$ un facteur irréductible de χ_u, alors $\deg P = 2$ (car u n'a pas de racine réelle). De plus, $\ker P(u)$ est stable par u et u^* (car u est normal). Remarquons deux choses :

— si $x \in \ker P(u)$ est non nul, alors $\mathrm{Vect}(x, u(x))$ est un espace stable (par u) de dimension 2.

— Si $\lambda \in \mathbb{C}$ est une valeur propre de u, alors [2] :

$$\ker(u - \lambda \,\mathrm{id}_E) = \ker\left(u^* - \overline{\lambda}\,\mathrm{id}_E\right)$$

Soit $v = u - \lambda\,\mathrm{id}_E$. On a $v^* = u^* - \overline{\lambda}\,\mathrm{id}_E$. Soit $x \in E$.

$$\begin{aligned} x \in \ker v &\iff v(x) = 0 \\ &\iff \langle\, v(x) \mid v(x)\,\rangle = 0 \\ &\iff \langle\, x \mid v^*v(x)\,\rangle = 0 \\ &\iff \langle\, x \mid vv^*(x)\,\rangle = 0 \\ &\iff \langle\, v^*(x) \mid *\, v(x)\,\rangle = 0 \\ &\iff x \in \ker v^* \end{aligned}$$

Soit $\lambda \in \mathbb{C}$ une valeur propre, et $w \in E$ un vecteur propre non nul associé à λ (vu comme point de l'espace E vu comme $\mathbb{C}$-espace vectoriel).

$$(uu^*)(x) = u(\overline{\lambda}x) = \lambda\overline{\lambda}x = |\lambda|^2 x$$

Ainsi, $|\lambda|^2$ est valeur propre uu^*. Soit x un vecteur propre associé à cette valeur propre, et soit $F = \mathrm{Vect}(x, u(x))$. Montrons que F est stable par u^*. On remarque que $F = \mathrm{Vect}(u(x), u^2(x))$, puis que $u^*u(x) = |\lambda|^2 x \in F$ et $u^*u^2(x) = |\lambda|^2 u(x) \in F$. Finalement, F et $F^\perp$ sont tous deux stables par u *et* par u^*. On conclut alors par récurrence.

□

Exemples.

— Endomorphismes autoadjoints : $u = u^*$. Alors toute valeur propre λ de u vérifie $\lambda = \overline{\lambda}$. Ainsi, un endomorphisme autoadjoint n'a que des valeurs propres réelles. On en déduit le *théorème spectral* : un endomorphisme autoadjoint est diagonalisable en base orthonormée.

— Endomorphismes unitaires (ou orthogonaux) : $uu^* = \mathrm{id}_E$. Pour toute valeur propre λ de u, alors $|\lambda|^2$ est valeur de $uu^* = \mathrm{id}_E$, donc $|\lambda| = 1$. Il existe alors une base orthonormée $\mathcal{B}$ telle que

$$\mathrm{mat}_{\mathcal{B}}(u) = \begin{pmatrix} \varepsilon_1 & & & & & \\ & \ddots & & & (0) & \\ & & \varepsilon_s & & & \\ & & & R(\theta_1) & & \\ & (0) & & & \ddots & \\ & & & & & R(\theta_r) \end{pmatrix} \quad \text{où } \varepsilon_i \in \{-1, 1\}, \text{ et } R(\theta_j) = \begin{pmatrix} \cos\theta_j & \sin\theta_j \\ -\sin\theta_j & \cos\theta_j \end{pmatrix}$$

On note $\mathcal{U}(E)$ le groupe des endomorphismes unitaires (pour la composition).

2. Plus généralement, pour tout $w \in \mathscr{L}(E)$, $\ker w = \ker w^*$ lorsque v est normal.

Proposition 5.2.1. *Soit $\|\cdot\|$ la norme subordonnée de la norme euclidienne. Alors, $\mathcal{U}(E)$ est compact.*

Démonstration. Pour tout $u \in \mathscr{L}(E)$ un endomorphisme unitaire et vecteur $x \in E$, alors $\|u(x)\|_2 = \|u^*(x)\|_2 = \|x\|_2$. On en déduit qu'un endomorphisme unitaire est de norme 1. Puis, $\mathcal{U}(E)$ est fermé comme image réciproque du singleton $\{1\}$ par l'application continue $u \mapsto uu^*$ (car u^* est polynomiale[3] en u). Or, $\mathscr{L}(E)$ est de dimension finie, donc $\mathcal{U}(E)$ est compact car fermé-borné. □

5.3 Décomposition polaire

Soit s un endomorphisme autoadjoint d'un espace E hermitien, alors $\langle x \mid s(x) \rangle \in \mathbb{R}$, pour tout $x \in E$. En effet, pour tout $x \in E$, $\langle x \mid s(x) \rangle = \langle s(x) \mid x \rangle = \overline{\langle x \mid s(x) \rangle}$.

Définition 5.3.1. *On dit que s est positif (resp. défini positif) si*

$$\forall x \in E,\ \langle x \mid s(x) \rangle \geq 0$$

$$\big(\text{resp. } \forall x \in E \backslash \{0_E\},\ \langle x \mid s(x) \rangle > 0\big)$$

On note $\mathcal{S}^+(E)$ l'ensemble des endomorphismes autoadjoints positifs, et $\mathcal{S}^{++}(E)$ l'ensemble des endomorphismes autoadjoints définis positifs.

Remarque. Si s est autoadjoint, alors s est positif *si et seulement si* toutes ses valeurs propres sont positives. Il est défini positif *si et seulement si* toutes ses valeurs propres sont strictement positives.

Lemme 5.3.1. *Soit $s \in \mathcal{S}^{++}(E)$, alors il existe un unique $\sigma \in \mathcal{S}^{++}(E)$ tel que $\sigma^2 = s$.*

Démonstration.

— Existence. On diagonalise u dans une base $\mathcal{B} = (e_1, \ldots, e_n)$ orthonormal. On a alors $\mathrm{mat}_{\mathcal{B}}(u) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ (avec $\lambda_i > 0$). On peut alors poser $\sigma(e_i) = \sqrt{\lambda_i} e_i$, et σ est autoadjoint, et vérifie $\sigma^2 = s$.

— Unicité. Remarquons que σ défini ainsi est un polynôme en s (on peut prendre P le polynôme interpolateur tel que $P(\lambda_i) = \sqrt{\lambda_i}$). Soit τ une racine de s, alors τ commute avec s, et donc avec $P(s) = \sigma$. σ et τ sont alors codiagonalisables dans une base $(b_1, \ldots, b_n)$. On a alors $\sigma(b_i) = \sqrt{\lambda_i} b_i$ et $\tau(b_i) = \mu_i b_i$. On a alors $\mu_i^2 = \lambda_i$. Or, les valeurs propres de s sont strictement positives, donc $\mu_i = \sqrt{\lambda_i}$. Donc σ et τ coïncident sur base $(b_1, \ldots, b_n)$, d'où $\sigma = \tau$.

□

3. En remarquant par exemple qu'un endomorphisme normal est inversible, et $u^* = u^{-1}$ peut alors s'écrire comme polynôme en u

Théorème 5.3.1. *Soit E un espace hermitien ou euclidien. L'application :*

$$\begin{array}{ccc} \mathcal{S}^{++}(E)\times\mathcal{U}(E) & \longrightarrow & \mathrm{GL}(E) \\ (s,\omega) & \longmapsto & s\circ\omega \end{array}$$

est un homéomorphisme.

Démonstration.

— Injectivité. Soit $(s,\omega)\in\mathcal{S}^{++}(E)\times\mathcal{U}(E)$, et $u=s\omega$. Alors $uu^*=s\omega(s\omega)^*=s\omega\omega^*s^*=s^2$. Alors nécessairement, s est l'unique racine carrée de $u\in\mathcal{S}^{++}(E)$, et $\omega=s^{-1}u$ est uniquement déterminé.

— Surjectivité. Soit s la racine carrée de $u\in\mathcal{S}^{++}(E)$. Alors, on pose $\omega=s^{-1}u$. On a alors $\omega\omega^*=s^{-1}uu^*(s^{-1})^*=s^{-1}s^2s^{-1}=\mathrm{id}_E$.

— Continuité. Montrons que $u\longmapsto(s,\omega)$ est continue. Soit $(u_k)_k$ une suite d'éléments de $\mathrm{GL}(E)$, convergeant vers u (pour la norme subordonnée de la norme euclidienne). On note $u_k=s_k\omega_k$ pour tout $k\in\mathbb{N}$. Il suffit de montrer que $s_k\longrightarrow s$ et $\omega_k\longrightarrow\omega$. On vérifie d'abord que $\mathcal{U}(E)$ est compact. $(\omega_k)_k$ admet une valeur d'adhérence ω_∞. Soit ϕ une extractrice telle que $\omega_{\phi(k)}\longrightarrow\omega_\infty$. Alors $s_{\phi(k)}\longrightarrow u\omega_\infty^{-1}$, et donc $s_\infty:=u\omega_\infty^{-1}\in\mathcal{S}^+(E)$. Or, s_∞ est inversible par composition, donc $s_\infty\in\mathcal{S}^+(E)$. Ainsi, u s'écrit $u=s_\infty\omega_\infty$ avec $s_\infty\in\mathcal{S}^{++}(E)$ et $\omega_\infty\in\mathcal{U}(E)$. Par injectivité de l'application que nous étudions, la valeur d'adhérence ω est unique, et donc $(\omega_k)_k$ converge. Il en est alors de même pour $(s_k)_k$, et nous avons montré la continuité de l'application réciproque.

□

Corollaire 5.3.1. *Soit E un espace euclidien, et G un sous-groupe compact de* $\mathrm{GL}(E)$ *contenant $\mathcal{O}(E)$. Alors $G=\mathcal{O}(E)$.*

Démonstration. Soit $g\in G$. On écrit $g=s\circ\omega$ avec $(s,\omega)\in\mathcal{S}^{++}(E)\times\mathcal{U}(E)$. On a $\omega\in\mathcal{O}(E)\subset G$. Ainsi, $s\in G$ et $s^{-1}\in G$. Or, la famille $(s^k)_{k\in\mathbb{Z}}$ est bornée car G est compact. Mais puisque $(s^k)_{k\in\mathbb{N}}$ est bornée, s n'a pas de valeur propre de module strictement plus grand que 1. Un même argument sur s^-1 montre que les valeurs propres de s sont exactement de module 1. Puisque que $s\in\mathcal{S}^{++}(E)$, on en déduit que toutes les valeurs propres de s valent 1, et donc $s=\mathrm{id}_E$.

□

Corollaire 5.3.2. *Deux matrices réelles sont orthogonalement semblables si et seulement si elles sont unitairement semblables.*

Corollaire 5.3.3. *Soit E un espace euclidien. L'enveloppe convexe de $\mathcal{O}(E)$ est la boule unité de $\mathscr{L}(E)$ (pour la norme subordonnée à la norme euclidienne).*

Démonstration. Soit B la boule unité de $\mathscr{L}(E)$ et C l'enveloppe convexe de $\mathcal{O}(E)$. On a déjà $C\subset B$ car la boule unité est convexe, et les éléments de $\mathcal{O}(E)$ sont de normes 1. Montrons maintenant l'inclusion réciproque. Une première remarque est que

$$C=\{v\in\mathscr{L}(E)\,|\,\forall\varphi\in E^*,\exists g\in(n),\ \varphi\circ v\leq g\circ v\}$$

□

Chapitre 6

Représentations et théorie des caractères

6.1 Représentations linéaires des groupes finis

Dans cette section, $\mathbb{K}$ désigne un corps et G un groupe.

6.1.1 Représentations de groupes

Définition 6.1.1 (Représentation linéaire)**.** *On appelle* ***représentation linéaire*** *de G la donnée (V, ρ), où V est un $\mathbb{K}$-espace vectoriel et $\rho : G \longrightarrow \mathrm{GL}(V)$ est un morphisme de groupes.*

Remarque. Une représentation de G est une action par applications linéaires. On transforme chaque élément du groupe G en une endomorphisme de V. On pourra par exemple noter $g \cdot x = \rho(g)(x)$, pour $g \in G$, et $x \in V$.

Définition 6.1.2 (Degré d'une représentation)**.** *Soit (V, ρ) une représentation de G. Si V est de dimension finie, on appelle* $\dim V$ *le degré de la représentation.*

Exemples.

— Si $V = \mathbb{K}$ et $\rho(g) = \mathrm{id}_{\mathbb{K}}$ pour tout $g \in G$, (V, ρ) est la représentation triviale.

— Si V est un $\mathbb{K}$-espace vectoriel, $(V, \mathrm{id}_{\mathrm{GL}(V)})$ est une représentation de $\mathrm{GL}(V)$.

— Une représentation de degré 1 de G est équivalent à la donné d'un morphisme $G \longrightarrow \mathbb{K}^\times$.

— Soit $n \in \mathbb{N}^*$. Si $G = \mathbb{Z}/n\mathbb{Z}$, alors $(\mathbb{K}, \rho)$ est une représentation, où $\rho(\overline{k}) = \omega^k$ (avec ω une racine n-ième de l'unité de $\mathbb{K}$).

— Si (V, ρ) est une représentation d'un groupe G et si H est un sous-groupe de G, alors $(V, \rho_{|H})$ est une représentation de H.

— Soit $V = \mathbb{K}[G]$ un espace vectoriel possédant une base indexée par G, $(e_g)_{g\in G}$. On peut définit l'action ρ par $\rho(g)(e_h) = e_{gh}$ pour tout $g, h \in G$.

— Plus généralement si G opère sur un ensemble X, on peut définir une représentation de G par $\mathbb{K}^{(X)}$. On peut définir $\rho(g)(\mathbb{1}_x) = \mathbb{1}_{g\cdot x}$ pour tout $(g, x) \in G \times X$, ce qui est suffisant puisqu'on définit $\rho(g)$ sur la base canonique de $\mathbb{K}^{(X)}$.

Définition 6.1.3 (Morphisme de représentations)**.** *Soient (V_1, ρ_1) et (V_2, ρ_2) des représentations de G. On appelle **morphisme de représentations** de V_1 vers V_2 une application linéaire $f \in \mathscr{L}(V_1, V_2)$ telle que :*

$$\forall g \in G,\ f \circ \rho_1(g) = \rho_2(g) \circ f.$$

Notation. On dit aussi que f est G**-équivariant**. On note $\mathrm{Hom}_G(V_1, V_2)$ l'ensemble des morphismes de représentations de V_1 vers V_2. On définit aussi la notion d'isomorphisme, d'endomorphisme, et d'automorphisme de représentations.

Exemples.

— Les homothéties sont des morphismes de représentations.

— Soit $f \in \mathrm{GL}(V)$, et $\tilde{\rho} : G \longrightarrow \mathrm{GL}(V)$, $g \longmapsto f \circ \rho(g) \circ f^{-1}$. Alors, $(V, \tilde{\rho})$ est une représentation, et f est un isomorphisme de (V, ρ) dans $(V, \tilde{\rho})$.

— Soit (V, ρ) une représentation de G, $x \in V$, et $(e_g)_{g \in G}$ une base de $\mathbb{K}[G]$. L'application f : $\mathbb{K}[G] \longrightarrow V$, $e_g \longmapsto \rho(g)(x)$ est G-équivariant.

Définition 6.1.4. *Soit (V, ρ) une représentation de G. On appelle sous-représentation de G la donnée d'un sous-espace vectoriel $W \subset V$ stable par $\rho(g)$ pour tout $g \in G$.*

Exemples.

— $\{0_V\}$ et V sont des sous-représentations de V.

— Supposons G abélien et $V = \mathbb{C}^n$. Les $\rho(g)$ ont une droite stable commune, donc V contient une sous-représentation de dimension 1 (car pour tout $g, h \in G$, $\rho(g) \circ \rho(h) = \rho(h) \circ \rho(g)$).

— Si $f_1 : (V_1, \rho_1) \longrightarrow (V_2, \rho_2)$ est G-équivariante, alors $\ker f$ et $\mathrm{Im}\, f$ sont des sous-représentations.

— Soit $\rho : G \longrightarrow \mathrm{GL}(\mathbb{K}^{(X)})$ la représentation donnée par $g \cdot e_x = e_{g \cdot x}$. Elle contient contient comme sous-représentation les sous-espaces $\mathrm{Vect}\{e_\omega \,|\, \omega \in \Omega\}$ où Ω est une orbite (ou une réunions d'orbite).

6.1.2 Répertoire des représentations classiques

Proposition 6.1.1. *Soit (V, ρ) une représentation et W une sous-représentation. Alors, V/W est muni d'une structure naturelle de représentation de G par*

$$g \cdot \pi(x) = \pi(g \cdot x)$$

pour tout $g \in G$ et $x \in V$, où $\pi : V \longrightarrow V/W$ est la projection canonique. De plus, π est G-équivariante.

Démonstration. Pour tout $g \in G$, W est stable par $\rho(g) \in \mathscr{L}(V)$. Le morphisme $\rho(g)$ induit donc bien un endomorphisme $\overline{rho(g)}$ sur V/W en passant au quotient. Ce morphisme vérifie bien que pour tout $x \in V$,

$$\overline{\rho(g)}(\pi(x)) = \pi(\rho(x))$$

par propriété du quotient. De plus, $\overline{\rho}$ est bien un morphisme puisque ρ l'est. Enfin, on a bien pour tout $(g, x) \in G \times V$,

$$g \cdot \pi(x) = \pi(g \cdot x)$$

ce qui signifie exactement que $\pi : (V, \rho) \longrightarrow (V/W, \overline{\rho})$.

$\square$

Définition 6.1.5. *Une représentation (V, ρ) est dite être une somme directe de sous-représentations s'il existe $W_1, \ldots, W_r$ des sous-représentations de V telles que*

$$V = \bigoplus_{i=1}^{r} W_i$$

Exxemple. Soient $V_1, \ldots, V_r$ des représentations de G. On muni $V = V_1 \times \cdots \times V_r$ de l'action définie pour tout $(x_1, \ldots, x_r) \in V$ par

$$g \cdot (x_1, \ldots, x_r) = (g \cdot x_1, \ldots, g \cdot x_r).$$

Cette représentation est somme directe des sous-représentations $W_i = f_i(V_i)$ où pour tout $x_i \in V_i$,

$$f_i(x_i) = (0, \ldots, 0, x_i, 0, \ \ldots, 0) \in \{0\}^{i-1} \times V_i \times \{0\}^{r-i}.$$

Proposition 6.1.2. *Soit (V, ρ) une représentation de G. Alors, V^* peut être muni d'une structure naturelle de représentation par*

$$(g \cdot \phi)(x) = \phi(g^{-1} \cdot x)$$

pour tout $g \in G$, $\phi \in V^*$, et $x \in V$. C'est-à-dire que $\rho^*(g) = {}^t\rho(g^{-1})$ pour tout $g \in G$.

Proposition 6.1.3. *Soit $(V_1, \rho_1), (V_2, \rho_2)$ des représentations de G. Alors, $V_1 \otimes V_2$ peut être muni d'une structure naturelle de représentation de G par*

$$g \cdot (x_1 \otimes x_2) = (g \cdot x_1) \otimes (g \cdot x_2)$$

pour tout $g \in G$, et $(x_1, x_2) \in V_1 \times V_2$. C'est-à-dire : $(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g)$, pour tout $g \in G$.

Proposition 6.1.4. *Soit $(V_1, \rho_1), (V_2, \rho_2)$ des représentations de G. Alors, $\mathscr{L}(V_1, V_2)$ peut être muni d'une structure naturelle de représentation de G par*

$$\forall g \in G, \forall u \in \mathscr{L}(V_1, V_2), \forall x \in V_1, \ (g \cdot u)(x) = g \cdot (u(g^{-1} \cdot x)).$$

C'est-à-dire : $(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g)$, pour tous $g \in G$.

Proposition 6.1.5. *Soit* $(V_1, \rho_1), (V_2, \rho_2)$ *des représentations de* G *de dimensions finies. Alors, l'isomorphisme naturel*

$$\begin{array}{rcl} V_1^* \otimes V_2 & \longrightarrow & \mathscr{L}(V_1, V_2) \\ \phi_1 \otimes x_2 & \longmapsto & \left| \begin{array}{rcl} V_1 & \longrightarrow & V_2 \\ x_1 & \longmapsto & \phi_1(x_1)x_2 \end{array} \right. \end{array}$$

induit un isomorphisme entre les représentations correspondantes.

6.1.3 Théorème de Maschke

Dans cette sous-section, on suppose G être un groupe fini et les représentations de degrés finis. On suppose de plus que le corps de base est $\mathbb{C}$.

Lemme 6.1.1. *Soient* (V_1, ρ_1), (V_2, ρ_2) *des représentations de* G *de degrés finis, avec* G *un groupe fini, et soit* $f \in \mathscr{L}(V_1, V_2)$. *L'application*

$$f_G : \left| \begin{array}{rcl} V_1 & \longrightarrow & V_2 \\ x & \longmapsto & \dfrac{1}{|G|} \displaystyle\sum_{g \in G} g f(g^{-1}x) \end{array} \right.$$

est G*-équivariante.*

Démonstration. Soit $g \in G$. Montrons que $f_G \circ \rho_1(g) = \rho_2(g) \circ f_G$. Soit $x \in V_1$, on a

$$\begin{array}{rcl} f_G(\rho_1(g)(x)) & = & \dfrac{1}{|G|} \displaystyle\sum_{h \in G} h f(h^{-1} \rho_1(g)(x)) \\ & = & \dfrac{1}{|G|} \displaystyle\sum_{h \in G} h f(\rho_1(h^{-1}g)(x)) \\ & = & \dfrac{1}{|G|} \displaystyle\sum_{h \in G} gh f(\rho_1((gh)^{-1}g)(x)) \\ & = & g \dfrac{1}{|G|} \displaystyle\sum_{h \in G} h f(\rho_1(h)^{-1}(x)) \\ & = & g \dfrac{1}{|G|} \displaystyle\sum_{h \in G} h f(h^{-1}x) = \rho_2(g)(f_G(x)) \end{array}$$

où le passage de la troisième à la quatrième ligne s'est effectué *via* le changement de variable (bien sûr bijectif) $h \mapsto gh$.

$\square$

Remarque. Le lecteur habitué à la théorie des actions n'aura aucun soucis pour écourter cette démonstration et éviter les détails superflus.

Théorème 6.1.1 (Maschke). *Soit (V, ρ) une représentation de degré fini de G, avec G un groupe fini. Soit $W \subset V$ une sous-représentation de G. Il existe une unique sous-représentation $W' \subset V$ de G telle que*

$$V = W \oplus W'.$$

Démonstration. Soit F un supplémentaire de W dans V, et soit p la projection sur W parallèlement à F. Soit enfin p_G l'application G-équivariante associée à p comme définie dans le lemme précédent. Puisque $p(V) \subset W$ et que W est une sous-représentation de G, on en déduit que $p_G(V) \subset W$. De plus, on remarque que $p_G(x) = x$ pour tout $x \in W$, ce qui permet au final d'affirmer que $p_G^2 = p_G$ (puisque $p(V) \subset W$). Ainsi p_G est un projecteur. On pose alors $W' = \ker p_G$ et alors, puisque p_G est un projecteur, on a

$$V = W \oplus W'.$$

□

Exemple. Soit $G = \mathbb{Z}/n\mathbb{Z}$.

Toute représentation de $\mathbb{Z}/n\mathbb{Z}$ est somme directe de sous-représentation de degré 1. En l'occurence, les représentations de degré 1 sont les $\rho_\omega : \overline{k} \longmapsto \omega^k$ avec ω une racine n-ième de l'unité. Alors,

$$\mathbb{C}[\mathbb{Z}/n\mathbb{Z}] \cong \bigoplus_{\omega \in \mathcal{U}_n(\mathbb{C})} \rho_\omega.$$

6.1.4 Décompositions en sous-espaces irréductibles

On supposera encore que G est un groupe fini, dont V est une représentation sur $\mathbb{C}$ de degré fini.

Définition 6.1.6. *Soit G un groupe fini, et (V, ρ) une représentation finie sur $\mathbb{C}$. On dit que V est irréductible si ses seules sous-représentations sont $\{0_V\}$ et V.*

Exemples.

- Les représentations de dimension 1 sont irréductibles.
- Si G est abélien, ses représentations sont tous de dimension 1.
- L'hyperplan d'équation $x_1 + \cdots + x_n = 0$ est une sous-représentation de la sous-représentation naturelle $\mathfrak{S}_n \longrightarrow \mathbb{C}$.

Proposition 6.1.6. *Soit (V, ρ) une représentation fini sur $\mathbb{C}$ de G, un groupe fini. Alors V se décompose en somme directe de sous-représentations irréductibles : il existe $V_1, \ldots, V_r$ des sous-représentations irréductibles de (V, ρ) telles que*

$$V = \bigoplus_{i=1}^{r} V_i.$$

Démonstration. Appliquer une récurrence forte sur $n = \deg V$ en utilisant le théorème de Maschke. $\square$

Lemme 6.1.2 (Schur)**.** *Soit G un groupe fini, et V_1, V_2 des représentations sur $\mathbb{C}$ de degrés finis. Si V_1 et V_2 sont irréductibles.*

(i) Si V_1 et V_2 sont isomorphes, alors $\mathrm{Hom}_G(V_1, V_2)$ est isomorphe à $\mathbb{C}$.

(ii) Si V_1 et V_2 ne sont pas isomorphes, alors $\mathrm{Hom}_G(V_1, V_2) = \{0_{\mathscr{L}(V_1,V_2)}\}$.

Démonstration. Soit $f : V_1 \longrightarrow V_2$ une application linéaire G-équivariante non nulle. Alors, $\ker f$ est une représentation distincte de V_1, donc par irréductibilité $\ker f = \{0_{V_1}\}$ et f est injective. De la même manière, on observe que $\mathrm{Im}\, f = V_2$ et f est en fait un isomorphisme. Cela montre alors que si V_1 et V_2 ne sont pas isomorphes, nécessairement f est nulle. Supposons maintenant V_1 et V_2 isomorphes. Quitte à étudier $g^{-1} \circ f$ où $g : V_2 \longrightarrow V_1$ est un isomorphisme, on peut supposer $V_1 = V_2$.

Soit $\lambda \in \mathbb{C}$ une valeur propre de f. Alors, $f - \lambda\, \mathrm{id}_{V_1}$ est un endomorphisme de représentations de V_1. Or, son noyau étant une sous-représentation de V_1, on a nécessairement que $f = \lambda\, \mathrm{id}_{V_1}$. Réciproquement, on vérifie que les homothéties sont bien G-équivariantes, ce qui démontre que $\mathrm{Hom}_G(V_1, V_2) = \mathbb{C} f$. $\square$

Proposition 6.1.7. *Soit V et W des représentations finies sur $\mathbb{C}$ d'un groupe fini G. Si W est irréductible, alors $\dim(\mathrm{Hom}_G(W, V))$ est le nombre de facteurs isomorphes apparaissant dans une décomposition de V en somme de sous-représentations irréductibles.*

Démonstration. $\square$

Notation. L'entier $\dim \mathrm{Hom}_G(V, W)$ s'appelle la *multiplicité* de W dans V. Elle est notée $\mu_{W,V}$.

Corollaire 6.1.1. *Soit V une représentation de G. On a*

$$V \cong \bigoplus_{\substack{W \subset V \\ \text{irréductible}}} W^{\oplus \mu_{W,V}}.$$

Remarque. Il faut bien comprendre ici que pour chaque $W \subset V$ irréductible tel que $\mu_{W,V} \neq 0$, il apparait dans la décomposition exactement $\mu_{W,V}$ espaces irréductibles tous isomorphes à W.

6.1.5 Exemple : le groupe diédral

Soit $n \in \mathbb{N}^*$. Le groupe diédral D_n est engendré par r et s où r est une rotation d'angle $\frac{2\pi}{n}$ et s la réflexion d'axe horizontal, ce qui assure que $srs = r^{-1}$. Soit alors (V, ρ) une représentation irréductible de D_n. On note $R = \rho(r)$ et $S = \rho(s)$. Soit $x \in V$ un vectuer propre pour R associé à la valeur propre ω. On a alors $Rx = \omega x$, et on en déduit que $\omega^n = 1$. Ainsi, $R(Sx) = \frac{1}{\omega} Sx$. On en déduit que $\mathrm{Vect}(x, Sx)$ est stable par $\rho(r)$ et $\rho(s)$ donc que $\mathrm{Vect}(x, Sx)$ est une sous-représentation de V. Or, V étant irréductible, on a $V = \mathrm{Vect}(x, Sx)$.

— Si $\deg V = 1$, alors $Sx = \pm x$, et alors $\omega^2 = 1$ (donc $\omega = 1$ si n est impair, et $\omega = \pm 1$ si n est pair).

— Si $\deg V = 2$, alors $\omega \in \{-1, 1\}$, et alors, si $\mathcal{B} = (x, Sx)$,

$$\begin{pmatrix} \omega & 0 \\ 0 & 1/\omega \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

6.2 Théorie des caractères

6.2.1 Caractères

Définition 6.2.1. *Soit (V, ρ) une $\mathbb{K}$-représentation de degré fini de G. On appelle* caractère *de la représentation V l'application*

$$\chi_V : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{K} \\ g & \longmapsto & \mathrm{Tr}(\rho(g)). \end{array} \right.$$

Propriétés et exemples.

— Si $V \cong V'$, alors $\chi_V = \chi_{V'}$.

— On a $\chi_V(e_G) = \deg V$ où 1_G désigne le neutre du groupe G.

— Si $V = \bigoplus_{i=1}^r V_i$, alors $\chi_V = \sum_{i=1}^r \chi_{V_i}$.

— Si $\deg V = 1$, $\chi_V = \rho$.

— Pour tout $W \subset V$, $\chi_{V/W} + \chi_W = \chi_V$.

— Pour tout $g \in G$,

$$\chi_{\mathbb{K}[G]}(g) = \begin{cases} |G| & \text{si } g = 1_G, \\ 0 & \text{sinon.} \end{cases}$$

— Soit V une représentation irréductible de degré 2 du groupe diédral D_n. Alors,

$$\chi_V(r) = 2\Re(\omega) \quad \text{et} \quad \chi_V(s) = 0.$$

— Si $\mathbb{K} = \mathbb{C}$, alors $\chi_{V^*} = \overline{\chi_V}$.

— Si $\mathbb{K} = \mathbb{C}$, alors $\chi_{\mathscr{L}(V,V')} = \overline{\chi_V}\chi_{V'}$.

6.2.2 Caractères irréductibles

On suppose maintenant que G est fini, $\mathbb{K} = \mathbb{C}$, et que les représentations sont de degré fini. Commençons cette sous-section par l'observation suivante.

$$\chi_V = \sum_{\substack{W \subset V \\ \text{irréductible}}} \mu_{W,V} \chi_W.$$

Une interrogation naturelle sera ici de se demander s'il est possible de retrouver les $\mu_{W,V}$ à partir de la seule donnée de χ_V.

Définition 6.2.2. *Un caractère est dit irréductible s'il est le caractère d'une certaine représentation irréductible.*

Lemme 6.2.1. *Soit V une représentation de G et soit*

$$V^G = \{x \in V \mid \forall g \in G,\, gx = x\}$$

l'ensemble des points fixes de l'action de G sur V. Alors, l'application

$$p : \left| \begin{array}{ccc} V & \longrightarrow & V \\ x & \longmapsto & \dfrac{1}{|G|} \displaystyle\sum_{g \in G} gx \end{array} \right.$$

est un projecteur sur V^G

Démonstration. On observe d'abord que p est bien linéaire[1] Soit $x \in V$. Si $x \in V^G$ alors clairement $p(x) = x$. Si maintenant $x \in V$, alors on observe en réindexant que pour tout $g \in G$, $p(x) = gp(x)$, ce qui signifie que $p(V) \subset V^G$ et donc que p est bien un projecteur sur V^G.

□

Corollaire 6.2.1. *Soit V une représentation de G. Alors,*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Démonstration. Puisque p est un projecteur, $\mathrm{rg}(p) = \mathrm{Tr}(p)$.

□

Exemple. Si $V = \mathbb{C}[G]$, $V^G = \mathrm{Vect}(e_g)_{g \in G}$.

6.2.3 Orthogonalité des caractères

On munit l'espace de fonctions $\mathbb{C}^G$ du produit scalaire défini pour tout $f_1, f_2 : G \longrightarrow \mathbb{C}$ par

$$\langle\, f_1 \mid f_2 \,\rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Lemme 6.2.2. *Soient V_1 et V_2 des représentations de G. On munit $\mathscr{L}(V_1, V_2)$ de sa structure naturelle de représentation de G. Alors,*

$$\mathrm{Hom}_G(V_1, V_2) = \mathscr{L}(V_1, V_2)^G.$$

1. sans oublier de se convaincre que V^G est bien un sous-espace vectoriel de V.

Démonstration. Soit $f \in \mathscr{L}(V_1, V_2)$. On remarque que $f \in \mathrm{Hom}_G(V_1, V_2)$ *si et seulement si* f est G-équivariante, *i.e* si pour tout $g \in G$,

$$\rho_2(g) \circ f = f \circ \rho_1(g).$$

Cela est encore équivalent à $\rho_2(g) \circ f \circ \rho_1(g)^{-1} = f$, *i.e* que $g \cdot f = f$ pour tout $g \in G$ au sens de la représentation de G par $\mathscr{L}(V_1, V_2)$.

□

Proposition 6.2.1. *Soient V_1 et V_2 des représentations de G. Alors,*

$$\dim \mathrm{Hom}_G(V_1, V_2) = \langle\, \chi_{V_1} \,|\, \chi_{V_2} \,\rangle\,.$$

Démonstration. On a

$$\begin{aligned} \dim(\mathrm{Hom}_G(V_1, V_2)) &= \dim \mathscr{L}(V_1, V_2)^G \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\mathscr{L}(V_1, V_2)}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g)\overline{\chi_{V_2}(g)} = \langle\, \chi_{V_1} \,|\, \chi_{V_2} \,\rangle\,. \end{aligned}$$

□

Corollaire 6.2.2. *Les caractères irréductibles de G forment une famille orthonormée.*

Remarque. Si

$$V \cong \bigoplus_{\substack{W \subset V \\ \text{irréductible}}} W^{\oplus \mu_{W,V}}, \quad \text{alors } \langle\, \chi_V \,|\, \chi_V \,\rangle = \sum_{\substack{W \subset V \\ \text{irréductible}}} \mu_{W,V}^2.$$

Corollaire 6.2.3. *Une représentation V de G est irréductible si et seulement si $\langle\, \chi_V \,|\, \chi_V \,\rangle = 1$.*

6.2.4 Application à la représentation régulière

Soit G un groupe fini, et $V = \mathbb{C}[G]$ sa représentation régulière.

Proposition 6.2.2. *Soit W une représentation irréductible de G. Alors, $\langle\, \chi_W \,|\, \chi_V \,\rangle = \deg W$.*

Démonstration. C'est une conséquence du fait que $\chi_V(g) = 0$ si $g \neq 1_G$, et $\chi_V(g) = |G|$ sinon.

□

Corollaire 6.2.4. *On a*

$$V = \bigoplus_{\substack{W \subset V \\ \text{irréductible}}} W^{\oplus \deg W}.$$

Corollaire 6.2.5. *On a*

$$|G| = \sum_{\substack{W \subset V \\ \text{irréductible}}} (\deg W)^2.$$

6.3 Fonctions centrales

6.3.1 Caractères et fonctions centrales

Définition 6.3.1. *Soit G un groupe. On appelle* ***fonction centrale*** *sur G toute application $f : G \longrightarrow \mathbb{C}$ invariante par conjugaison, i.e que pour tout $g, h \in G$,*

$$f(ghg^{-1}) = f(h).$$

Exemples.

— Les indicatrices de classes de conjugaisons sont des fonctions centrales.

— Les caractères de représentations sont des fonctions centrales.

Proposition 6.3.1. *Les caractères irréductibles forment une base orthonormée de l'espace des fonctions centrales.*

Démonstration. La famille des caractères irréductible est nécessairement libre puisqu'elle est orthonormée.

□

6.3.2 Table de caractères