

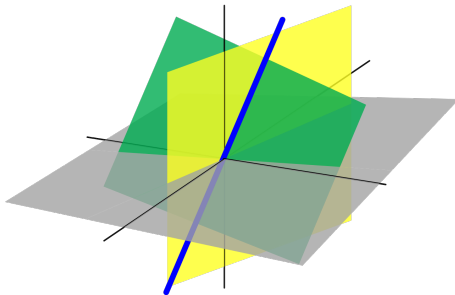
ALGÈBRE LINÉAIRE

COURS DU 12 DÉCEMBRE

Jérôme Scherer

ttpoll.eu

041603



7.1.3 THÉORÈME SPECTRAL

THÉORÈME SPECTRAL

Soit A une matrice symétrique. Alors

- 1 A admet n valeurs propres réelles (avec multiplicité).
- 2 Pour toute valeur propre λ on a $\text{mult}(\lambda) = \dim E_\lambda$.
- 3 Si $\lambda \neq \mu$, alors $E_\lambda \perp E_\mu$.
- 4 A est orthodagonalisable.

ATTENTION !

Si λ est une valeur propre de multiplicité ≥ 2 , alors la base de vecteurs propres de E_λ fournie par la méthode de Gauss n'est pas orthogonale en général, il faut **Gram-Schmidter** pour obtenir une base orthonormée de vecteurs propres.

7.1.4 EXEMPLE

$$A = \begin{pmatrix} 4 & 1 & 3 & 1 \\ 1 & 4 & 1 & 3 \\ 3 & 1 & 4 & 1 \\ 1 & 3 & 1 & 4 \end{pmatrix}$$

$$\text{et } C_A(t) = \dots =$$

$$= (1-t)^2 \begin{vmatrix} 4-t & 1 & 3 & 1 \\ 1 & 4-t & 1 & 3 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{vmatrix} \begin{array}{l} C_1 + C_3 \\ = \\ C_2 + C_4 \end{array} = (1-t)^2 \begin{vmatrix} 7-t & 2 & 3 & 1 \\ 2 & 7-t & 1 & 3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$$\begin{aligned} & \stackrel{\text{dév. } L_3}{=} (1-t)^2 \cdot 1 \cdot \begin{vmatrix} 7-t & 2 & 1 \\ 2 & 7-t & 3 \\ 0 & 0 & 1 \end{vmatrix} \stackrel{\text{dév.}}{=} (1-t)^2 \begin{vmatrix} 7-t & 2 \\ 2 & 7-t \end{vmatrix} = \\ & = (1-t)^2 (t^2 - 14t + \underbrace{49 - 4}_{45}) \stackrel{\text{Vie}}{=} (1-t)^2 (t-5)(t-9). \end{aligned}$$

On a trois valeurs propres 5, 9 et 1 avec $\text{mult}(1) = 2$.

$$E_5 = \text{Vect} \left\{ \begin{pmatrix} -1/2 \\ 1/2 \\ -1/2 \\ 1/2 \end{pmatrix} \right\}, \quad E_9 = \text{Vect} \left\{ \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} \right\} \quad \begin{array}{l} \text{on vérifie} \\ E_5 \perp E_9. \end{array}$$

On doit encore calculer E_1 et trouver une base orthonormée de E_1 pour orthogonaliser A .

7.1.4 EXEMPLE, FIN

$$E_1 = \text{Ker}(A - I_4) = \text{Ker} \begin{pmatrix} 3 & 1 & 3 & 1 \\ 1 & 3 & 1 & 3 \\ 3 & 1 & 3 & 1 \\ 1 & 3 & 1 & 3 \end{pmatrix} = \text{Ker} \begin{pmatrix} 3 & 1 & 3 & 1 \\ 1 & 3 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$L_1 - 3L_2 \quad L_2 - 3L_1' \quad L_1 \cdot (-\frac{1}{8})$$

$$= \text{Ker} \begin{pmatrix} 0 & -8 & 0 & -8 \\ 1 & 3 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \text{Ker} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} =$$

$$\text{Vect} \left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\} = \text{Vect} \left\{ \begin{pmatrix} -\sqrt{2}/2 \\ 0 \\ \sqrt{2}/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -\sqrt{2}/2 \\ 0 \\ \sqrt{2}/2 \end{pmatrix} \right\}$$

↑
orthogonaux! on normalise

On obtient une base orthonormée de vecteurs propres

$$B = \left(\begin{pmatrix} -\sqrt{2}/2 \\ 0 \\ \sqrt{2}/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -\sqrt{2}/2 \\ 0 \\ \sqrt{2}/2 \end{pmatrix}, \begin{pmatrix} -1/2 \\ 1/2 \\ -1/2 \\ 1/2 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} \right), \quad U = \begin{pmatrix} -\sqrt{2}/2 & 0 & -1/2 & 1/2 \\ 0 & -\sqrt{2}/2 & 1/2 & 1/2 \\ \sqrt{2}/2 & 0 & -1/2 & 1/2 \\ 0 & \sqrt{2}/2 & 1/2 & 1/2 \end{pmatrix}$$

$$U^{-1} = U^T \quad \text{et} \quad U^T A U = \text{diag}(1, 1, 5, 9)$$

7.1.5 MÉTHODE.

- ❶ Vérifier que A est symétrique.
- ❷ Calculer $c_A(t)$ et en extraire les racines (valeurs propres).
- ❸ Calculer les espaces propres. Pour chacun, le procédé de Gram-Schmidt donne une base orthonormée.
- ❹ En rassemblant les bases des espaces propres on obtient une base orthonormée $\mathcal{U}$ de $\mathbb{R}^n$.
- ❺ La matrice P dont les colonnes sont les vecteurs $\vec{u}_i$ de $\mathcal{U}$ est orthogonale et $P^T A P$ est diagonale.

AVANTAGE

La matrice de changement de base inverse est P^T .

7.1.6 MATRICE DE PROJECTION

Soit $\vec{u}$ un vecteur unitaire ^{de $\mathbb{R}^n$} et $A = \vec{u} \vec{u}^T$. Alors

$$A\vec{x} = \vec{u}(\vec{u}^T \vec{x}) = (\vec{u} \cdot \vec{x}) \vec{u}$$

- 1 $\vec{u}$ est un vecteur propre de A pour la valeur propre 1 car $(\vec{u} \cdot \vec{u}) \vec{u} = \vec{u}$.
- 2 Posons $W = \text{Vect}(\vec{u})$. Alors $W^\perp$ est le noyau de A .
- 3 Ainsi $E_1 = W$ et $E_0 = W^\perp$.

PROPOSITION

La matrice $A = \vec{u} \vec{u}^T$ est la matrice de la projection orthogonale sur $W = \text{Vect}(\vec{u})$. On a $A\vec{x} = \text{proj}_{\vec{u}} \vec{x}$.

C'est un cas particulier que nous avons vu pour UU^T , matrice de projection orthogonale quand les colonnes de U sont orthonormées.

7.1.6 EXAMPLES

$$\textcircled{1} \quad \vec{u} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\vec{u} \vec{u}^T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

projection
orthogonale
sur Ox

$$\textcircled{2} \quad \vec{u} = \begin{pmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{pmatrix}$$

$$\vec{u} \vec{u}^T = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

sw $x=y$

③ $\vec{u} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$$\vec{u} \vec{u}^T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

pas une
matrice de
projection.

C'est en fait la projection de ② suivie d'une homothétie de rapport 2.

$$\text{Proj}_{\text{Osc}}: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$(\text{proj}_{\text{fox}})_{\mathcal{C}_R} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\text{proj}: \mathbb{R}^2 \longrightarrow W$$

$$(proj_{\partial x})_{e_n} = \begin{pmatrix} ? \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^{1 \times 2}$$

7.1.7 DÉCOMPOSITION SPECTRALE

DÉFINITION

Soit A symétrique, U orthogonale et $U^T A U = D$ diagonale.

L'ensemble des valeurs propres de A est appelé **spectre** de A .

$$\begin{aligned} A &= U D U^T = (\vec{u}_1 \ \vec{u}_2 \ \dots \ \vec{u}_n) \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix} \begin{pmatrix} \vec{u}_1^T \\ \vec{u}_2^T \\ \vdots \\ \vec{u}_n^T \end{pmatrix} \\ &= (\lambda_1 \vec{u}_1 \ \dots \ \lambda_n \vec{u}_n) \begin{pmatrix} \vec{u}_1^T \\ \vdots \\ \vec{u}_n^T \end{pmatrix} = \lambda_1 \vec{u}_1 \vec{u}_1^T + \dots + \lambda_n \vec{u}_n \vec{u}_n^T \end{aligned}$$

$A = \lambda_1 \vec{u}_1 \vec{u}_1^T + \dots + \lambda_n \vec{u}_n \vec{u}_n^T$

 est la **décomposition spectrale**.

7.1.7 INTERPRÉTATION DE LA DÉC. SPECTRALE

Si A est une matrice symétrique, alors

$$A = \lambda_1 \vec{u}_1 \vec{u}_1^T + \cdots + \lambda_n \vec{u}_n \vec{u}_n^T$$

est sa décomposition spectrale.

Ainsi A se décompose en une combinaison linéaire de projections orthogonales !

7.1.7 EXEMPLE DE DÉC. SPECTRALE

Soit $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ la matrice symétrique que nous avons orthodiagonalisée mardi. Nous avons trouvé une base orthonormée de vecteurs propres (pour les valeurs propres -1 et 3) :

$$\mathcal{U} = (\vec{u}_1, \vec{u}_2) = \left(\begin{pmatrix} -\sqrt{2}/2 \\ \sqrt{2}/2 \end{pmatrix}, \begin{pmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{pmatrix} \right)$$

La décomposition spectrale de A est donc

$$A = -1 \cdot \vec{u}_1 \vec{u}_1^T + 3 \cdot \vec{u}_2 \vec{u}_2^T$$

7.1.7 EXEMPLE, SUITE

$$\text{Ici } \overline{u}_1 \overline{u}_1^T = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}$$

la proj. orthogonale
sur la droite $x = -y$

$$\overline{u}_2 \overline{u}_2^T = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

_____ $x = y$

$$A = -1 \cdot \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix} + 3 \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}.$$

A.12 EXEMPLES ET PREUVE

- ① $\text{car } \mathbb{F}_2 = 2$ et $\text{car } \mathbb{F}_p = p$, premier
- ② $\text{car } \mathbb{F}_4 = 2$
- ③ $\text{car } \mathbb{R} = 0$ $n \cdot 1 \neq 0$

Lemme.

Dans un corps K , si $x, y \neq 0$, alors $x \cdot y \neq 0$

preuve. On montre que si $x \cdot y = 0$, alors x ou y est nul. Supposons que l'un des deux est non nul, disons que c'est x . On doit prouver : $y = 0$.

Comme $x \neq 0$, x^{-1} existe. Alors

$\downarrow$
0 absorbant

$$0 = x^{-1} \cdot 0 = x^{-1} \cdot (xy) \stackrel{\text{ass.}}{=} (x^{-1}x)y = 1_K y = y. \quad \square$$

A.12 PREUVE, SUITE ET FIN

Soit K un corps fini et $n = \text{car}(K) \in \mathbb{N}^*$

On montre que si $n = a \cdot b$, alors a ou $b = 1$.

Comme $n \neq 1$ car $1 \cdot 1_K = 1_K \neq 0_K$, n sera donc premier.

$$\begin{aligned} 0 &= n \cdot 1_K = a \cdot b \cdot 1_K = \underbrace{1_K + \dots + 1_K}_{\leftarrow a \cdot b \rightarrow} = \\ \text{distr.} \quad &= (\underbrace{1_K + \dots + 1_K}_{\leftarrow a \rightarrow}) \cdot (\underbrace{1_K + \dots + 1_K}_{\leftarrow b \rightarrow}) = (a \cdot 1_K) \cdot (b \cdot 1_K) \end{aligned}$$

Par le lemme, soit $a \cdot 1_K = 0$, soit $b \cdot 1_K = 0$.

Or n est le plus petit entier non nul tq $n \cdot 1_K = 0$.

Donc soit $a = n$ et $b = 1$, soit $b = n$ et $a = 1$.

□

A.13 LA CARDINALITÉ D'UN CORPS FINI

Soit $p = \text{car}K$. Alors le corps $\mathbb{F}_p$ agit sur K par multiplication.

DÉFINITION

Soit $k \in \mathbb{F}_p$ et $x \in K$. On pose $k \cdot x = (k \cdot 1_K) \cdot x$.

Cette action est bien définie puisque $p \cdot 1_K = 0$. Les propriétés de l'action sont toutes conséquence du fait que K est un corps.

PROPOSITION

Soit K un corps fini et $p = \text{car}K$. Alors K est un $\mathbb{F}_p$ -espace vectoriel.

THÉORÈME

Soit K un corps fini et $p = \text{car}K$. Alors il existe n tel que K a p^n éléments. On appelle ce nombre la **cardinalité** de K .

A.13 PREUVE

Si K est fini, $\dim_{\mathbb{F}_p} K < \infty$ et on peut choisir une base $\mathcal{B}$ qui a n éléments. Le passage en coordonnées $(\)_{\mathcal{B}} : K \longrightarrow (\mathbb{F}_p)^n$
 $x \longmapsto (x)_{\mathcal{B}}$

C'est une bijection si bien que la cardinalité de K est la même que celle de $(\mathbb{F}_p)^n$. Celle-ci vaut p^n . $\square$

Exemples:

$$\text{Card}(\mathbb{F}_p) = p$$

$$\text{Card}(\mathbb{F}_4) = 2^2$$

$$\text{Card}(K) = 6 \text{ est impossible.}$$

A.14 CONSTRUCTION DE CORPS FINIS

La construction de $\mathbb{F}_4$ n'est pas un cas isolé, la méthode générale fonctionne de la même manière. Soit p un nombre premier.

- 1 Trouver un polynôme $p(t)$ unitaire irréductible de degré n dans $\mathbb{F}_p[t]$.
- 2 Considérer l'ensemble K de tous les restes de division par $p(t)$. Il y en a p^n .
- 3 Définir la somme dans K comme dans $\mathbb{F}_p[t]$.
- 4 Définir le produit dans K par celui de $\mathbb{F}_p[t]$, **modulo** $p(t)$.
- 5 Alors K est un corps de cardinalité p^n .

A.15 EXEMPLE : LE CORPS $\mathbb{F}_{49}$

Nous cherchons un polynôme irréductible de degré 2.

PROPOSITION

Soit K un corps et $p(t) = t^2 - a$. Si a n'est pas un carré, alors $p(t)$ est irréductible. *dans K*

Preuve. En effet $p(t)$ est irréductible si et seulement si il n'a pas de racine (car il est de degré 2), si et seulement si $p(x) \neq 0$ pour tout $x \in K$.

Or, $p(x) = x^2 - a = 0$ si et seulement si $a = x^2$ est un carré. $\square$.

REMARQUE

Pour trouver un polynôme irréductible de degré 2 à coefficients dans $\mathbb{F}_7$, nous cherchons à comprendre quels éléments sont des carrés.

A.15 LES CARRÉS DE $\mathbb{F}_7$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

Par exemple 3 n'est pas un carré dans $\mathbb{F}_7$,
donc $t^2 - 3$ est irréductible.

$\mathbb{F}_4[t]$ est l'ensemble des restes de la division par $t^2 - 3$
 $= \{ a \cdot t + b \mid a, b \in \mathbb{F}_7 \}$

Somme: $(3t + 2) + (3t + 5) = 6t + 7 = 6t = \underline{\underline{-t}}$

Produit: $(t + 1)(t + 4) = t^2 + 5t + 4 = 3 + 5t + 4$
 $= \underline{\underline{5t}}$

$$\begin{array}{r} t^2 + 5t + 4 \quad | \quad t^2 - 3 \\ -(t^2 - 3) \quad | \quad 1 \\ \hline 5t + 7 = 5t \end{array}$$

$$t^2 - 3 = 0$$

A.15 CALCULS DANS $\mathbb{F}_{49}$

On pose $\alpha = [\epsilon]$ et comme $[\epsilon^2 - 3] = 0$
dans $\mathbb{F}_{49}$
 $\alpha^2 = 3$

$$\mathbb{F}_{49} = \{ a \cdot \alpha + b \mid a, b \in \mathbb{F}_7 \}$$

Le produit est déterminé par $\boxed{\alpha^2 = 3}$

A.15 LA NOTION DE CLASSE

Nous avons construits $\mathbb{F}_p$ comme le corps des restes de la division euclidienne des entiers $\mathbb{Z}$ par p , un nombre premier. Chaque entier dont le reste de la division vaut 2 représente alors dans $\mathbb{Z}$ le même élément dans $\mathbb{F}_p$:

$$\dots, 2 - 2p, 2 - p, 2, 2 + p, 2 + 2p, \dots$$

On dit que le reste 2 est la **classe** de tous ces nombres, on écrit souvent $[2] \in \mathbb{F}_p$ pour distinguer cet élément du nombre entier 2.

Dans $\mathbb{F}_{49}$, l'élément α est la classe $[t]$. C'est un élément qui est représenté dans $\mathbb{F}_7[t]$ par tous les polynômes dont le reste de la division par $t^2 - 3$ vaut t , par exemple

$$t^2 + t + 3, t^3 + 5t, \dots$$

A.16 QUELQUES FAITS SANS PREUVE

PROPOSITION

Soit p un nombre premier et $n \geq 1$ un entier. Il existe toujours un polynôme irréductible de degré n dans $\mathbb{F}_p[t]$.

THÉORÈME

Soit p un nombre premier et $n \geq 1$ un entier. Il existe toujours un corps fini de cardinalité p^n .

REMARQUE

En fait un tel corps est unique à isomorphisme près, ce qui signifie que deux choix différents de polynômes $p(t)$ et $q(t)$ donnent des corps $\mathbb{F}_p[t]/(p(t))$ et $\mathbb{F}_p[t]/(q(t))$ qui sont isomorphes.

Il existe donc un isomorphisme $f: \mathbb{F}_p[t]/(p(t)) \rightarrow \mathbb{F}_p[t]/(q(t))$.