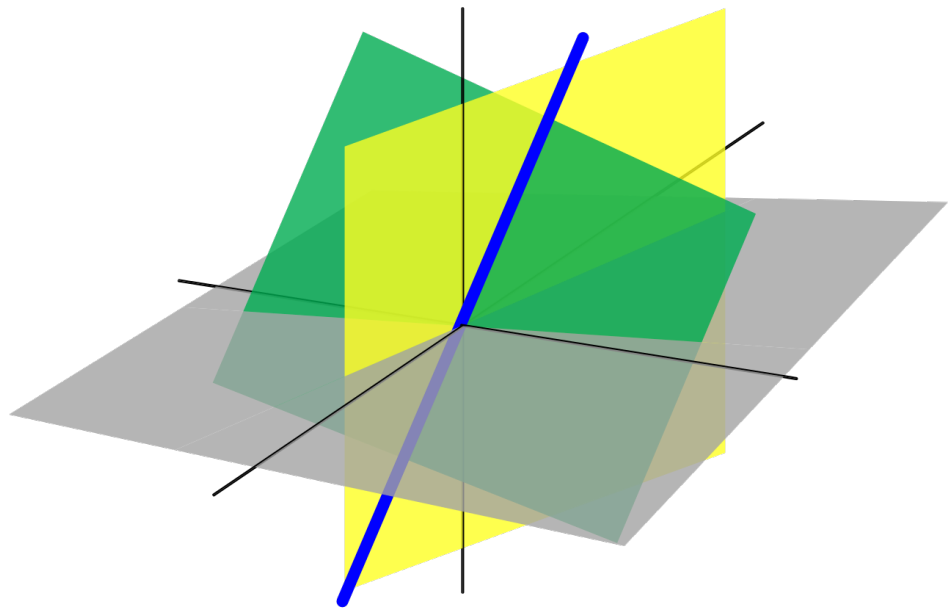
Algèbre Linéaire

Cours du 21 novembre

ttpoll.eu
634255

Jérôme Scherer



5.3.1 Diagonalisation

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Définition

Une matrice est diagonalisable si elle est semblable à une matrice diagonale, i. e. il existe P inversible telle que $P^{-1}AP$ est diagonale.

Théorème

Une matrice A de taille $n \times n$ est diagonalisable si et seulement si il existe une base $\mathcal{B}$ de $\mathbb{R}^n$ formée de vecteurs propres de A.

Preuve. On regarde A comme la matrice de $T : \mathbb{R}^n \to \mathbb{R}^n$ dans la base canonique : $T\vec{x} = A \cdot \vec{x}$ et $(T)^{\mathcal{C}an}_{\mathcal{C}an} = A$.

Soit $\mathcal{B}$ une autre base. Alors $(T)^{\mathcal{B}}_{\mathcal{B}}$ est diagonale $\iff$

$T(\vec{b}_i) = \lambda_i \vec{b}_i$

$\iff (T(\vec{b}_i))_{\mathcal{B}} = \lambda_i \vec{e}_i$. Dans la base $\mathcal{B}$ les coordonnées de $T(\vec{b}_i)$ sont nulles sauf la i-ème.

5.3.2 Observations

Soit A la matrice d'une application linéaire T exprimée dans la base canonique, $A = (T)^{\mathcal{C}an}_{\mathcal{C}an}$. Soit D la matrice de T exprimée dans une base $\mathcal{B}$, de sorte que $D = (T)^{\mathcal{B}}_{\mathcal{B}}$ est diagonale.

1. Les colonnes de la matrice de changement de base $P = (\mathrm{Id})^{\mathcal{C}an}_{\mathcal{B}}$ sont les vecteurs propres de la base $\mathcal{B}$.
2. $A = PDP^{-1}$ et D est diagonale, les valeurs propres $\lambda_1, \ldots, \lambda_n$ de A se trouvent dans la diagonale, dans l'ordre choisi pour construire la base.
3. Le déterminant de A est le produit des valeurs propres (avec multiplicité). En effet

$$\begin{aligned} \det A = & \quad \det(PDP^{-1}) = \det P \det D \det(P^{-1}) \\ = & \quad \det D = \lambda_1 \cdot \lambda_2 \cdot \cdots \cdot \lambda_n \end{aligned}$$

5.3.2 Exemple

Soit $T : M_{2\times 2}(\mathbb{R}) \to M_{2\times 2}(\mathbb{R})$ l'application linéaire définie par

$$T\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+d & b-c \\ c-b & a+d \end{pmatrix}$$

On commence par écrire la matrice de T dans la base canonique.

Cette matrice est de taille 4×4 !

$\mathcal{C}_{an} = (e_{11}, e_{12}, e_{21}, e_{22})$

$T(e_{11}) = T\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\mathcal{C}_{an}} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

$$A = (T)^{\mathcal{C}_{an}}_{\mathcal{C}_{an}} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

On calcule $C_A(t)$

5.3.2 Exemple, suite

On calcule le polynôme caractéristique

$$c_A(t) = \begin{vmatrix} 1-t & 0 & 0 & 1 \\ 0 & 1-t & -1 & 0 \\ 0 & -1 & 1-t & 0 \\ 1 & 0 & 0 & 1-t \end{vmatrix} \begin{matrix} \\ \\ L_4 \leftarrow L_4 + L_1 \\ = \\ L_3 \leftarrow L_3 + L_2 \\ \\ \end{matrix} \begin{vmatrix} 1-t & 0 & 0 & 1 \\ 0 & 1-t & -1 & 0 \\ 0 & -t & -t & 0 \\ 2-t & 0 & 0 & 2-t \end{vmatrix}$$

Lin de l. 1 pour L3 puis L4

$$= t\cdot(2-t) \begin{vmatrix} 1-t & 0 & 0 & 1 \\ 0 & 1-t & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ C_1 \leftarrow C_4 \\ = \\ C_2 \leftarrow C_3 \end{matrix}$$

$$= t\cdot(2-t) \begin{vmatrix} -t & 0 & 0 & 1 \\ 0 & 2-t & -1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \text{dév.} \\ = -t\cdot(2-t)\cdot t \\ C_1 \end{matrix} \begin{vmatrix} 2-t & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

5.3.2 Exemple, fin

$$= -t \cdot (2-t) \cdot t \cdot (2-t)(-1) \cdot 1$$

$$= t^2 (2-t)^2.$$

Deux valeurs propres $0, 2$, $\text{mult}(0) = 2$, $\text{mult}(2) = 2$

$$E_0 = \text{Ker } A = \text{Vect}\left\{ \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\}$$

rang 2

$$E_2 = \text{Ker}(A - 2I_4) = \text{Ker} \begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} =$$

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

Les 4 vecteurs propres de A forment une base de $\mathbb{R}^4$ qui permet de diagonaliser A. Pour diagonaliser T, on choisit une base de $\mathcal{M}_{2\times 2}(\mathbb{R})$

$$\mathcal{B} = \left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

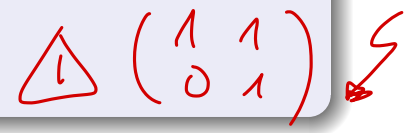
5.3.2 Exemple, fin

$$\left(\overline{T}\right)_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

5.3.3 Premier critère de diagonalisation

Théorème

Soit A une matrice de taille $n \times n$ ayant n valeurs propres distinctes. Alors A est diagonalisable.



Preuve. Pour chaque valeur propre on a un vecteur propre. Ces n vecteurs sont libres par 5.1.5 et forment alors une base de $\mathbb{R}^n$. □

Proposition

Soient λ et μ deux valeurs propres distinctes de A. Alors $E_\lambda \cap E_\mu = \{\overrightarrow{0}\}$.

Preuve. Soit $\overrightarrow{x} \in E_\lambda \cap E_\mu$, alors $A\overrightarrow{x} = \lambda\overrightarrow{x}$, et aussi $A\overrightarrow{x} = \mu\overrightarrow{x}$. Comme $\mu \neq \lambda$, alors $\overrightarrow{x} = \overrightarrow{0}$. □

Remarque

Les espaces propres E_λ et E_μ forment une somme directe $E_\lambda \oplus E_\mu$.

5.3.4 Multiplicités

Proposition

Soit λ une valeur propre de A. Alors $1 \leq \dim E_\lambda \leq \text{mult}(\lambda)$.

Preuve. E_λ contient un vecteur propre, non nul : $1 \leq \dim E_\lambda$.

5.3.4 Multiplicités

Proposition

Soit λ une valeur propre de A. Alors $1 \leq \dim E_\lambda \leq \text{mult}(\lambda)$.

Preuve. E_λ contient un vecteur propre, non nul : $1 \leq \dim E_\lambda$. Si $\overrightarrow{b}_1, \ldots \overrightarrow{b}_k$ est une base de E_λ, on peut la compléter en une base de $\mathbb{R}^n$.

5.3.4 Multiplicités

Proposition

Soit λ une valeur propre de A. Alors $1 \leq \dim E_\lambda \leq \text{mult}(\lambda)$.

Preuve. E_λ contient un vecteur propre, non nul : $1 \leq \dim E_\lambda$. Si $\overrightarrow{b}_1, \ldots \overrightarrow{b}_k$ est une base de E_λ, on peut la compléter en une base de $\mathbb{R}^n$. Dans cette base la matrice devient

$$\begin{pmatrix} \lambda & 0 & 0 & * & * \\ 0 & \ddots & 0 & * & * \\ 0 & 0 & \lambda & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \end{pmatrix}$$

Le polynôme caractéristique de cette matrice est le même que celui de A et commence par $(\lambda - t)^k$. Donc $k \leq \text{mult}(\lambda)$. □

5.3.5 Critère de diagonalisation

Les deux propositions ci-dessus sont les clés de notre deuxième critère. Il faut qu'il y ait assez de valeurs propres réelles et assez de vecteurs propres.

Théorème

Une matrice A est diagonalisable (sur $\mathbb{R}$) si et seulement si

1. Le polynôme caractéristique est scindé : il se décompose en produit de facteurs $(\lambda - t)$ avec des $\lambda \in \mathbb{R}$.

5.3.5 Critère de diagonalisation

Les deux propositions ci-dessus sont les clés de notre deuxième critère. Il faut qu'il y ait assez de valeurs propres réelles et assez de vecteurs propres.

Théorème

Une matrice A est diagonalisable (sur $\mathbb{R}$) si et seulement si

1. Le polynôme caractéristique est scindé : il se décompose en produit de facteurs $(\lambda - t)$ avec des $\lambda \in \mathbb{R}$.
2. Pour tout λ, on a $\dim E_\lambda = \text{mult}(\lambda)$.

Si A est diagonalisable on forme une base de vecteurs propres en réunissant les vecteurs de base de chaque espace propre.

5.3.5 Exemple

① $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $\quad c_A(t) = \begin{vmatrix} -t & 1 \\ -1 & -t \end{vmatrix} = t^2 + 1$

irréductible sur $\mathbb{R}$. Pas assez de valeurs propres réelles

A n'est pas diagonalisable sur $\mathbb{R}$.

Sur $\mathbb{C}$, $t^2 + 1 = (t - i)(t + i)$, A est diagonalisable

② $B = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$, $c_B(t) = (t-3)^2$. Il y a assez de valeurs propres : $\lambda = 3$, $\text{mult}(3) = 2$.

$E_3 = \text{Ker}\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ est de dim 1 par le Thm du rang

Pas assez de vecteurs propres, B n'est pas diagonalisable ni sur $\mathbb{R}$, ni sur $\mathbb{C}$.

Déf : mult géom de λ $=$ $\dim E_\lambda$.

A.1 Les corps : Définition

Jusqu'ici nous avons développé des méthodes qui permettent de travailler avec des matrices à coefficients dans $\mathbb{R}$ et nous avons aussi constaté que cela fonctionne dans $\mathbb{Q}$. Il y a beaucoup d'autres *corps de nombres* ! Vous connaissez bien sûr les nombres complexes, $\mathbb{C}$, et on pourrait refaire la théorie de la diagonalisation sur les complexes, nous en verrons d'autres.

Définition

Un corps K est un ensemble muni d'une addition $+$ et d'une multiplication $\cdot$ pour lesquelles les règles de calcul "usuelles" s'appliquent.

A.1 Les corps : Définition

Plus précisément on demande que

1. $(K, +)$ est un groupe abélien : il vérifie les axiomes d'associativité, de commutativité, il y a un élément neutre 0 et chaque nombre x admet un opposé $-x$.
2. Le produit est associatif, commutatif, il existe un élément neutre 1 et chaque nombre $x \neq 0$ admet un inverse x^{-1}. $1 \neq 0$
3. La multiplication est distributive par rapport à l'addition : $x(y + z) = xy + xz$ pour tous $x, yz \in K$.

A.2 Exemple : le corps $\mathbb{F}_2$

Soit $\mathbb{F}_2 = \{0, 1\}$. On définit somme et produit par les tables :

$+$	0	1
0	0	1
1	1	0

1 est l'opposé de 1

$\cdot$	0	1
0	0	0
1	0	1

Remarque

La symétrie des tableaux montre la commutativité des opérations.

Pour $+$ la ligne de 0 montre que c'est un élément neutre et pour $\cdot$ c'est celle de 1 qui le prouve.

A.3. Application : le code de Hamming

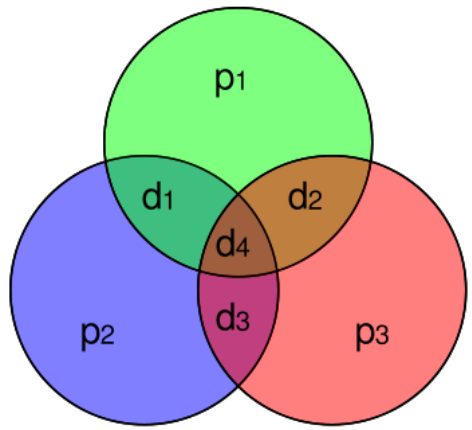
En 1946 l'ingénieur Hamming invente le premier code autocorrecteur pour ordinateurs à cartes perforées.

Son idée est d'ajouter à chaque mot de 4 bits $d_1 d_2 d_3 d_4$ dans $(\mathbb{F}_2)^4$ un mot de 3 bits de contrôle formé par les sommes dans $\mathbb{F}_2$:

1. $d_1 + d_2 + d_4$
2. $d_1 + d_3 + d_4$
3. $d_2 + d_3 + d_4$

A.3. Le code de Hamming

On utilise 16 signes comme alphabet de base : 0000, 0001, . . . , 1110, 1111. On visualise les bits de contrôle p_1, p_2 et p_3 comme suit :



Si une erreur se glisse dans la transmission, le code est capable de s'autocorriger. Si le mot $d_1 d_2 d_3 d_4 p_1 p_2 p_3 = 1001010$ est transmis, la parité de $d_1 + d_2 + d_4$ est correcte, mais les deux autres sont erronés. Ainsi il faut corriger le seul nombre commun aux bits de contrôle p_2 et p_3 qui n'apparaît pas dans p_1.

A.4 Le corps des nombres complexes

On utilise la notation cartésienne pour introduire $\mathbb{C}$.

Définition

Le corps des nombres complexes $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ est muni

1. de la somme $(a + bi) + (c + di) = (a + c) + (b + d)i$;
2. du produit $(a + bI)(c + di) = (ac - bd) + (ad + bc)i$.

Remarque

L'addition est définie coefficient par coefficient, pas de surprise ! La mutliplication est définie de la seule manière possible pour que

1. elle étende le produit de $\mathbb{R}$;
2. on ait $i^2 = -1$;
3. le produit soit distributif par rapport à la somme.

A.5 Les matrices de taille 2×2

1. On peut additionner deux matrices de même taille et $(M_{2\times 2}(\mathbb{R}), +)$ forme un groupe commutatif.
2. On peut aussi multiplier deux matrices 2×2 entre elles, ce produit est distributif par rapport à la somme, mais les matrices ne forment pas un corps !

Problèmes

Le produit n'est pas commutatif, mais pire, il existe de nombreuses matrices qui ne sont pas inversibles. L'ensemble des matrices de taille 2×2 forme ce que l'on appelle un anneau (non commutatif).

Par contre, il existe des sous-ensembles de $M_{2\times 2}(\mathbb{R})$ qui sont des corps !

A.6 Sous-anneaux des matrices de taille 2×2

1. Soit $S = \{A \in M_{2\times 2}(\mathbb{R}) \mid A \text{ est scalaire } \}$. Alors S forme un corps pour la somme et le produit de matrices. En fait l'application $f : \mathbb{R} \to S$ définie par $f(a) = aI_2$ est un isomorphisme qui identifie S avec le corps des nombres réels.
2. Soit $M = \{A \in M_{2\times 2}(\mathbb{R}) \mid a_{11} = a_{22} \text{ et } a_{12} = -a_{21}\}$. Alors M forme un corps.

Puisque la somme est associative et commutative et que le produit est associatif et distributif pour toutes les matrices, on vérifie seulement la commutativité du produit dans M et l'existence d'un inverse pour tout élément non nul de M.

A.6 M EST UN CORPS

$$\Pi = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

① A part $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, élément neutre pour $+$, toutes les matrices ont un inverse : $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 \geq 0$

$\det = 0$ ssi $a = b = 0$.

② Dans Π la multiplication est commutative !

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \underbrace{\begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}}_{\in \Pi} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\cdot\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Conclusion : $(\Pi, +, \cdot)$ est un corps. En fait on a un isomorphisme

$$f : \mathbb{C} \longrightarrow \Pi$$
$$a + bi \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$f(z \cdot z') = f(z) \cdot f(z')$, $f(z + z') = f(z) + f(z')$

$f(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

A.7 Arithmétique modulaire

Comme pour $\mathbb{F}_2 = \{0, 1\}$ on peut considérer l'ensemble des nombres entiers $\{0, 1, 2, \ldots, n-1\}$.

On regarde ces nombres comme tous les restes possibles de la division par n, ce qui nous permet de définir une somme et un produit en calculant dans $\mathbb{Z}$, mais en ne gardant que le reste de la division. Ainsi

1. Dans $\{0, 1, 2\}$ on calcule $2 + 2 =$ 1
2. Dans $\{0, 1, 2\}$ on calcule $2^3 =$
3. Dans $\{0, 1, 2, 3, 4\}$ on calcule $3 \cdot 4 =$
4. Dans $\{0, 1, 2, 3, 4\}$ on calcule $1 - 4 =$
5. Dans $\{0, 1, 2, 3, \ldots, 10, 11\}$ on calcule $10 \cdot 6 =$