

Algebre Lineaire II

David Wiedemann

Table des matières

1	Polynomes	4
1.1	Division avec reste	6
1.2	Factorisation des polynomes sur un corps	7
1.3	Factorisation des polynomes sur un corps	8
1.4	Diviseurs Communs le plus grand	8
1.5	Factorisation en elements irreductibles	10
2	Valeurs et Vecteurs Propres	11
3	Le polynome caracteristique	14
3.1	Theoreme de Cayley-Hamilton	15
4	Formes Bilineaires	17
4.1	Orthogonalite	18
4.2	Orthogonalite	19
4.3	Matrices congruentes	20
4.4	Formes Bilineaires symmetriques definies positives	20
4.5	La methode de Gram Schmidt	22
4.6	La methode des moindres carres	24
4.7	Formes sesquilineaires et produits hermitiens	25

List of Theorems

1	Definition (Centre d'un anneau)	4
2	Definition (Diviseurs de 0)	4
3	Definition (Anneau integre)	4
1	Theorème	4
4	Definition (Polynome)	4
2	Theorème	4
5	Definition (Degre d'un polynome)	5
3	Theorème	5

4	Theorème	5
5	Theorème	6
6	Corollaire	6
7	Theorème	6
6	Definition (Diviseurs de polynomes)	7
7	Definition (Racine)	7
8	Theorème	7
8	Definition (Multiplicite d'une racine)	8
9	Theorème (Theoreme fondamental de l'algebre)	8
9	Definition (Polynome irreductible)	8
10	Theorème	8
11	Theorème	8
10	Definition (Polynome Unitaire)	8
11	Definition (Diviseur Commun)	9
12	Theorème	9
12	Definition (PGCD)	9
13	Theorème (Algorithme d'Euclide)	9
14	Theorème	10
15	Theorème (La factorisation est unique)	10
16	Corollaire	11
13	Definition (Vecteur propre)	11
17	Lemme	11
14	Definition	11
18	Corollaire	12
15	Definition (Matrices semblables)	12
16	Definition (Sous-espace propre)	12
19	Lemme	12
20	Corollaire	13
17	Definition (Multiplicite algebrique)	14
21	Proposition	14
22	Theorème (Theoreme de diagonalisation)	14
23	Theorème (Evaluation d'une matrice dans un polynome)	15
24	Theorème (Cayley-Hamilton)	15
18	Definition (Polynome minimal)	16
25	Corollaire	16
19	Definition (Forme Bilineaire)	17
26	Proposition	17
20	Definition (Orthogonalite)	18
21	Definition (Complement orthogonal)	18
27	Proposition	18
28	Lemme	18

22	Definition (Matrices Congruentes)	18
23	Definition (Base orthogonale)	19
29	Lemme	19
30	Theorème	19
31	Lemme	20
24	Definition (Formes Bilineaires definies positives)	20
25	Definition (Norme d'un vecteur)	21
26	Definition	21
32	Proposition	21
33	Theorème (Theoreme de Pythagore)	21
34	Proposition (Regle du parallelogramme)	21
35	Theorème (Inegalite Cauchy-Schwarz)	22
36	Theorème (Inegalite triangulaire)	22
37	Lemme	22
38	Corollaire	23
27	Definition	24
39	Corollaire	24
40	Theorème	24
41	Theorème	25
28	Definition (Produit Hermitien)	25
29	Definition (Matrice hermitienne)	26
42	Proposition	26
30	Definition (Matrices Complexes congruentes)	26
43	Theorème	26
44	Theorème (Theoreme Spectral)	27
45	Lemme	27
46	Corollaire	27

1 Polynomes

Definition 1 (Centre d'un anneau)

Le centre $Z(R)$ est l'ensemble des elements x satisfaisant

$$\{x \in R \mid ra = ar \forall a \in R\}$$

Definition 2 (Diviseurs de 0)

a est un element non nul d'un anneau R satisfaisant qu'il existe $b \in R$ tel que $ab = 0$ ou $ba = 0$.

Definition 3 (Anneau integre)

Si un anneau est commutatif et n'a pas de diviseurs de 0, alors l'anneau est integre.

Theorème 1

Soit R un anneau, alors il existe un anneau $S \supseteq R$ (R est un sous-anneau) et $\exists x \in S \setminus R$ tel que

- $ax = xa, \forall a \in R$
- Si $a_0 + \dots + a_n x^n = 0$ et $a_i \in R \forall i$ alors $a_i = 0 \forall i$

Cet x est appele indeterminee ou variable.

Definition 4 (Polynome)

Un polynomer sur R est une expression de la forme

$$p(x) = a_0 + \dots + a_n x^n$$

ou a_i est le i -eme coefficient de $p(x)$.

$R[x]$ est l'ensemble des polynomes sur R .

Theorème 2

$R[X]$ est un sous-anneau. R est sans diviseurs de 0 $\Rightarrow R[X]$ est sans diviseurs de 0.

De meme, si R est commutatif, $R[x]$ aussi.

Preuve

Soit $f(x) = \sum a_i x_i, g(x) = \sum b_i x^i$ de degre n resp. m .

$$f(x) + g(x) = \sum_{i=1}^{\max(m,n)} (a_i + b_i) x^i$$

De meme, on a

$$f(x) \cdot g(x) = a_0 b_0 + \dots = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

Donc $R[X]$ est stable pour $+$, \cdot et donc immédiatement pour $-$, donc $R[X]$ est un sous-anneau de S .

Soient $f(x), g(x) \neq 0$ et $n = \max \{i : a_i = 0\}$, le $m + n$ -ième coefficient de $f(x)g(x)$ est $a_n b_m$ et donc si R est intègre, $R[x]$ l'est aussi. \square

Definition 5 (Degré d'un polynôme)

Soit $f(x) = a_0 + \dots \in R[X]$, $f(x) \neq 0$. On définit

$$\deg(f) = \max \{i : a_i \neq 0\}$$

Ce dernier terme s'appelle le coefficient dominant de f , de plus on définit

$$f(x) = 0 : \deg(f) = -\infty$$

Si $\deg(f) = 0$, alors f est une constante.

Theorème 3

Soit R un anneau, $f, g \in R[X] \neq 0$ tel que au moins un de leur coefficients dominants de f ou de g ne sont pas des diviseurs de 0. Alors $\deg(f \cdot g) = \deg(f) + \deg(g)$

Preuve

Soit $f(x) = a_0 + \dots, g(x) = b_0 + \dots, \deg f = n, \deg g = m$. Le $n + m$ ième coefficient de $f \cdot g = a_n \cdot b_m \neq 0$ \square

Soit $p(x) \in R[x]$, ce polynôme induit une application $f_p : R \rightarrow R$, on écrit aussi $p(r)$

Theorème 4

Soit K un corps et $r_0, r_1, \dots, r_n \in K$ des éléments distincts et soient $g_0, \dots, g_n \in K$.

Il existe un seul polynôme $f \in K[x]$ tel que

1. $\deg f \leq n$
2. $f(r_i) = g_i$

Preuve

On cherche a_0, \dots, a_n tel que

$$a_0 + a_1 r_i + \dots + a_n r_i^n = g_i$$

Donc, on cherche

$$\begin{pmatrix} 1 & r_0 & \dots & r_0^n \\ \vdots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \dots \end{pmatrix} = \begin{pmatrix} g_0 \\ \dots \end{pmatrix}$$

Il faut donc montrer que la matrice ci-dessus a un déterminant non nul.
 On le montre par induction sur n .
 Dans le cas $n = 0$, le déterminant vaut trivialement 1. Dans le cas $n > 0$, on a

$$\det \begin{pmatrix} 1 & 0 & \dots \\ 1(r_1 - r_0) & \dots & \\ \dots & \ddots & \\ 1(r_n - r_0) & \dots & \end{pmatrix} = (r_1 - r_0)(r_2 - r_0) \dots \det(V(r_1, \dots, r_n)) \neq 0 \quad \square$$

Lecture 2: Polynomes

Wed 24 Feb

Theorème 5

Soit K un corps fini de caractéristique q , alors $K \supseteq \mathbb{Z}_q$.
 De plus K est un espace vectoriel de \mathbb{Z}_q de dimension finie.

Corollaire 6

Soit K un corps infini. Deux polynomes sont égaux si et seulement si leurs évaluations sont les memes.

Preuve

Une direction est triviale.

L'autre suit immédiatement du theoreme 1.6 □

1.1 Division avec reste

Theorème 7

Soit R un anneau, $f, g \in R[x], g \neq 0$ et soit le coefficient de $g \in R^*$
 Il existe $q, r \in R[x]$ uniques tel que

1. $f(x) = q(x)g(x) + r(x)$
2. $\deg r < \deg g$

Preuve

Si $\deg f < \deg g$, on a fini.

Soit donc $\deg f \geq \deg g$, donc

$$f(x) = a_0 + \dots + a_n x^n$$

et

$$g(x) = b_0 + \dots + b_m x^m$$

et b_m^{-1} existe.

On procede par induction sur n .

Si $n = m$:

On note que

$$f(x) - \frac{a_n}{b_m}g(x)$$

est un polynome de degre $< n$ Si $n > m$:

On note que

$$f(x) - \frac{a_n}{b_m}x^{n-m}g(x)$$

est un polynome de degre $< n$.

Par hypothese d'induction il existe $q(x), r(x)$ tel que

- $f(x) - \frac{a_n}{b_m}x^{n-m}g(x) + r(x)$
- $\deg r < \deg g$

et donc on a fini de montrer l'existence.

Supposons maintenant qu'il existe r' et q' satisfaisant les memes proprietes que q et g , alors on a

$$q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$$

Donc

$$r' \neq r \text{ et } q' \neq q$$

□

en comparant les degre, on a une contradiction.

1.2 Factorisation des polynomes sur un corps

Definition 6 (Diviseurs de polynomes)

Soit $q(x) \in K[x]$.

q divise f si il existe $g(x)$ tel que

$$q(x)g(x) = f(x)$$

On dit que q est un diviseur de f , on ecrit $q(x)|f(x)$

Definition 7 (Racine)

Soit $p(x) \in K[x]$, et soit $\alpha \in K$ tel que $p(\alpha) = 0$

Theorème 8

Soit $f(x) \in K[x] \setminus \{0\}$, alors $\alpha \in K$ est une racine de f si et seulement si $(x - \alpha)|f(x)$

Preuve

Si $(x - \alpha)q(x) = f(x)$, alors on a fini.

sinon, la division de $f(x)$ par $x - \alpha$ avec reste donne

$$f(x) = q(x)(x - \alpha) + r \text{ ou } r \in K$$

Si $r \neq 0$, alors $f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r \neq 0$ et donc $(x - \alpha)|f(x)$

□

Definition 8 (Multiplicite d'une racine)

La multiplicite d'une racine α de $p(x) \in K[x]$ est le plus grand $i \geq 1$ tel que

$$(x - \alpha)^i | p(x)$$

Theorème 9 (Theoreme fondamental de l'algebre)

Tout polynome $p(x) \in \mathbb{C}[x] \setminus \{0\}$ de degre ≥ 1 possede une racine complexe.

Lecture 3: Factorisation des polynomes sur un corps

Tue 02 Mar

1.3 Factorisation des polynomes sur un corps

Soit K un corps.

Definition 9 (Polynome irreductible)

Un polynome $p(x) \in K[x] \setminus \{0\}$ est irreductible si

- $\deg p \geq 1$
- si $p(x) = f(x) \cdot g(x)$, alors $\deg f = 0$ ou $\deg g = 0$.

Theorème 10

Un polynome de degre 2 sur $K[x]$ est irreductible si et seulement si le polynome ne possede pas de racines.

1.4 Diviseurs Communs le plus grand**Theorème 11**

Soient $f(x), g(x) \in K[x]$ pas tous les deux nuls.

On considere l'ensemble $I = \{u \cdot f + v \cdot g : u, v \in K[x]\}$.

Il existe un polynome $d(x) \in K[x]$ satisfaisant

$$I = \{h \cdot d : h \in K[x]\}$$

Preuve

Soit $a \in I \setminus \{0\}$ de degre minimal.

L'ensemble $\{h \cdot d : h \in K[x]\}$ est clairement un sous-ensemble de I .

Il reste a montrer l'inclusion inverse.

Si d ne divise pas $uf + vg$, la division avec reste donne

$$uf + vg = qd + r \iff r = uf + vg - qd = (u - qu')f + (v - qv')g$$

Or le reste est non nul, mais le reste est de degre inferieur a $\deg d$. \nmid \square

Definition 10 (Polynome Unitaire)

Un polynome $f(x) \in K[x]$ dont le coeff. dominant = 1 est un polynome unitaire.

Definition 11 (Diviseur Commun)

Soient $f, g \in K[x]$ non-nuls.

Un diviseur commun de f et g est un polynome qui divise f et g .

Theorème 12

Soient $f, g \in K[x]$ non-nuls.

Soit $d \in K[x]$ comme dans le theoreme precedent.

- d est un diviseur commun de f et g .
- Chaque diviseur commun de f et g est un diviseur de d .
- Si d est unitaire, alors d est unique.

Preuve

- $f \in I \Rightarrow \exists h$ tel que $hd = f \iff d|f$ et $g \in I \Rightarrow d|g$
- Soit $d' \in K[x]$ tq $d'|f, d'|g$, on veut montrer que $d'|d$.

$$f = f'd', g = g'd'$$

des que $d \in I$, il existe $u, v \in K[x]$ tel que

$$d = uf + vg = uf'd' + vg'd' = (uf' + vg')d' \Rightarrow d'|d \quad \square$$

- Soit $d' \in I$ tel que $I = \{hd' | h \in K[x]\}$.
Soient d, d' unitaires.
 $d|d'$ et $d'|d$, donc ils sont les memes a un facteur pres.

Definition 12 (PGCD)

L'unique polynome unitaire $d \in K[x]$ qui satisfait les conditions ci-dessus est appele le plus grand commun diviseur de f et g .

Theorème 13 (Algorithme d'Euclide)

Soient f_0, f_1 non nuls et

$$\deg f_0 \geq \deg f_1$$

On cherche $\gcd(f_0, f_1)$ Si $f_1 = 0$, alors $\gcd = f_0$.

Si $f_1 \neq 0$ On pose

$$f_0 = q_1 f_1 + f_2$$

Soit $h \in K[x] : h|f_0$ et $h|f_1 \Rightarrow h|f_2$ Et donc on pose $\gcd(f_0, f_1) = \gcd(f_1, f_2)$ On repete jusqu'a trouver un f_k nul.

Grace a l'algorithme d'Euclide, on peut aussi trouver $u, v \in K[x]$ tel que $uf_0 + vf_1 = \gcd(f_0, f_1)$.

En effet, on a

$$\begin{pmatrix} f_i \\ f_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} f_{i-1} \\ f_i \end{pmatrix}$$

et donc en appliquant cette matrice plusieurs fois, on trouve une dépendance linéaire entre f_{k-1} et f_k

Et donc le $\gcd(f_0, f_1) = \frac{1}{\text{coeff dominant de } f_{k-1}}(uf_0 + vf_1)$

Lecture 4: Polynomes 2

Wed 03 Mar

1.5 Factorisation en éléments irréductibles

Un polynome $p(x)$ est irréductible si le degré de p est ≥ 1 , $p(x) \neq 0$.

Si $h|p$, alors $h = a$ ou $h = a \cdot p$.

Tout $f(x) \in K[x]$ se laisse factoriser

$$f(x) = a \prod_i p_i(x), p_i(x) \text{ irréductibles, unitaires}$$

Est-ce que cette factorisation est unique ?

Theorème 14

Soit $p(x) \in K[x] \setminus \{0\}$ irréductible et supposons que $p|f_1(x) \dots f_k(x)$, alors il existe i tel que $p(x)|f_i(x)$

Preuve

Par récurrence, il suffit de démontrer l'assertion pour $k = 2$.

Supposons que $p|f \cdot g$, $f, g \in K[x] \setminus \{0\}$.

Si $p \nmid f$, alors $\gcd(p, f) = 1$. Donc, il existe $u, v \in K[x]$ tel que $up + vf = 1$, donc on a

$$upg + vfg = g \Rightarrow p|upg + vfg \Rightarrow p|g \quad \square$$

Theorème 15 (La factorisation est unique)

La factorisation est unique à l'ordre près des p_i .

Preuve

Soit $f(x) = a \prod p_i(x)$ et $f(x) = a \prod q_j(x)$ une autre factorisation en éléments irréductibles.

Par récurrence sur k .

Si $k = 1$, alors

$$ap_1(x) = aq_1(x) \dots q_l(x)$$

Et donc $q_1(x) = p_1(x)$, car p_1 est irréductible. Si $k > 1$,

$$ap_1(x) \dots p_k(x) = aq_1(x) \dots q_l(x)$$

Grace au théorème ci-dessus, $p_1|q_j$ pour un certain $j \iff p_1 = q_j$. Et donc on obtient

$$p_2(x) \dots = q_1(x) \dots q_l(x) \quad \square$$

Par récurrence, cette factorisation existe et est la même à l'ordre près.

Corollaire 16

Soit $f(x) \in K[x] \setminus \{0\}$ et $\alpha_1 \dots$ des racines de f de multiplicité k_1, \dots, k_l respectivement.

Alors il existe $g(x) \in K[x]$ tel que

$$f(x) = g(x) \prod (x - \alpha_i)^{k_i}$$

Preuve

Exercice

□

2 Valeurs et Vecteurs Propres

Definition 13 (Vecteur propre)

Soit V un espace vectoriel sur K et f un endomorphisme sur V .

Un vecteur propre de f associe à la valeur propre $\lambda \in K$ est un vecteur $v \neq 0$ satisfaisant

$$f(v) = \lambda v$$

Lemme 17

Soit $B = \{v_1, \dots, v_n\}$ une base de V et $A \in K^{n \times n}$ la matrice de l'endomorphisme f relatif à B .

La matrice A est une matrice diagonale

$$A = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$$

$\iff v_i$ est un vecteur propre associé à la valeur propre λ_i .

Preuve

On a

$$[f(v_i)]_B = Ae_i = \lambda_i e_i$$

Donc v_i est un vecteur propre associé à λ_i .

Dans l'autre sens, les arguments sont similaires.

□

Definition 14

Un endomorphisme f sur un espace vectoriel de dimension finie est appelé diagonalisable s'il existe une base tel que $\{v_1, \dots\}$ de V composée de vecteurs propres.

Lecture 5: Vecteurs/Valeurs Propres

Tue 09 Mar

Corollaire 18

Soit $f : V \rightarrow V$ un endomorphisme et $\{v_1, \dots, v_n\}$ une base de V .
 Alors f est diagonalisable si et seulement si il existe une matrice inversible $P \in K^{n \times n}$ tel que $P^{-1}A_BP$ est diagonale.

Preuve

f est diagonalisable $\iff \exists B' = \{w_1, \dots\}$ tel que $A_{B'}$ est diagonale.

Mais $A_{B'} = P^{-1}A_BP$ □

Definition 15 (Matrices semblables)

$A, B \in K^{n \times n}$ sont semblables s'il existe $P \in K^{n \times n}$ inversible tel que

$$P^{-1}AP = B$$

Donc si f est diagonalisable, la matrice de f est semblable a une matrice diagonale.

Definition 16 (Sous-espace propre)

Soit $f : V \rightarrow V$ un endomorphisme et λ une valeur propre de f , alors

$$E_\lambda = \ker(f - \lambda \cdot \text{Id})$$

est l'espace propre de f associe a λ .

$\dim E_\lambda$ est la multiplicite geometrique de λ .

Lemme 19

Soit $f : V \rightarrow V$ un endomorphisme et v_1, \dots, v_r des vecteurs propres associes aux valeurs propres $\lambda_1, \dots, \lambda_r$ distinctes.
 Alors $\{v_1, \dots, v_r\}$ est un ensemble libre.

Preuve

$r = 1$ est evident.

Pour $r = 2$:

Supposons que v_1, v_2 sont lineairement dependants, alors il existe $\exists \alpha_1, \alpha_2 \in K \setminus \{0\}$ tel que

$$\alpha_1 v_1 + \alpha_2 v_2 = 0$$

Spg $\lambda_2 \neq 0$, en appliquant f , on trouve

$$0 = \alpha_1 f(v_1) + \alpha_2 f(v_2)$$

$$0 = \alpha_1 \frac{\lambda_1}{\lambda_2} v_1 + \alpha_2 v_2$$

$$0 = \alpha_1 \left(1 - \frac{\lambda_1}{\lambda_2}\right) v_2$$

Pour $r > 2$

Supposons l'assertion est fausse et soit $r > 2$ minimal tel que v_1, \dots, v_r

sont lin. dependants.. Soit

$$\alpha_1 v_1 + \dots = 0$$

avec $\alpha_i \neq 0 \forall i$, alors

$$0 = \alpha_1 \frac{\lambda_1}{\lambda_r} v_1 + \dots + \alpha_r v_r$$

En soustrayant les deux egalites, on trouve

$$0 = \alpha_1 \left(1 - \frac{\lambda_1}{\lambda_r}\right) v_1 + \dots$$

□

Ce qui contredit la minimalite.

Corollaire 20

Soit $f : V \rightarrow V$ un endomorphisme de V sur K et $\dim V = n$.

Soient λ_1, \dots , les valeurs propres differentes de f .

Soit $n_1 \dots$ les multiplicites geometriques respectives.

Soient $B_i = \{v_1^{(i)}, \dots, v_{n_i}^{(i)}\}$ des bases de E_{λ_i} , alors

$$\bigcup_i B_i$$

est un ensemble libre.

f est diagonalisable $\iff n_1 + \dots + n_r = n$

Preuve

Soit

$$\sum_{i=1}^r \sum_{j=1}^{n_i} \alpha_{ij} v_j^{(i)} = 0$$

□

Montrons que $\alpha_{ij} = 0 \forall i, j$ "Immediat" par lemme d'avant.

On remarque immediatement que si $\sum n_i = n$, les vecteurs propres forment une base.

A l'inverse, soit f diagonalisable, cad il existe une base B de V composee de vecteurs propres. Soit $m_i = |B \cap E_{\lambda_i}|$, donc m_i est le nombre de vecteurs dans B associe a λ_i .

Clairement $\sum m_i = n$, mais $m_i \leq n_i \leq \dim E_{\lambda_i}$, donc $\sum n_i = n$.

3 Le polynome caractéristique

Soit A une matrice $n \times n$, $\lambda \in K$ est une valeur propre de l'endomorphisme défini par A si et seulement si $\ker(A - \lambda \text{Id}) \supsetneq \{0\}$. On note

$$\det(A - \lambda I) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^n (A - \lambda \text{Id})_{i\pi(i)}$$

On observe que λ est une valeur propre de f si et seulement si λ est une racine de p_A .

Soit $f : V \rightarrow V$ un endomorphisme, $B = \{v_1, \dots\}$ une base de V . Le polynome caractéristique de f est donné par

$$\det(A_B - \lambda \text{Id})$$

Cette définition fait du sens, car le changement de base n'influence pas la valeur du déterminant.

Definition 17 (Multiplicité algébrique)

La multiplicité algébrique d'une valeur propre est la multiplicité comme racine du polynome caractéristique.

Proposition 21

Soit f un endomorphisme de $V \rightarrow V$.

Soit $\lambda \in K$ une valeur propre.

La multiplicité géométrique de λ est au plus la multiplicité algébrique.

Preuve

Soit $\{v_1, \dots, v_r\}$ une base de E_λ , on complète cette base en une base de V avec $\{w_1, \dots, w_{n-r}\}$. Dans cette base, la représentation de la matrice de $A - \lambda \text{Id}$ implique que

$$\det(A - x \text{Id}) = (\lambda - x)^r \det C \quad \square$$

et donc r est au plus la multiplicité algébrique.

Theorème 22 (Théorème de diagonalisation)

Soit V un espace vectoriel sur K de dimension n , $f : V \rightarrow V$ un endomorphisme $\lambda_1, \dots \in K$ les valeurs propres distinctes, alors f est diagonalisable si et seulement si

- $p_f(x) = (-1)^n \prod_{i=1}^r (x - \lambda_i)^{g_i}$
- $\dim E_{\lambda_i} = g_i$ pour tout i

Preuve

Soit f diagonalisable et soit $B = \{v_1, \dots\}$ une base composee de vecteurs propres. A_B est une matrice diagonale, alors $p_f(x) = \det(A_B - x \text{Id}) = (-1)^n \prod (\lambda_i - x)^{g_i}$.

De plus $\dim(\ker(A_B - \lambda_i \text{Id})) = g_i$

Soient m_i les multiplicites geometriques des valeurs propres.
car

$$\deg(p_f) = n$$

on a fini. □

Lecture 7: Cayley-Hamilton

Tue 16 Mar

3.1 Theoreme de Cayley-Hamilton

Theoreme 23 (Evaluation d'une matrice dans un polynome)

Soit $p(x) = a_0 + \dots + a_n x^n \in K[x]$ Pour $A \in K^{n \times n}$, on definit

$$p(A) = a_0 \text{Id} + \dots + a_n A^n$$

Theoreme 24 (Cayley-Hamilton)

Soit $A \in K^{n \times n}$ et $p(\lambda) \in K[\lambda]$ le polynome caracteristique de A , alors $p(A) = 0 \in K^{n \times n}$

Preuve

Supposons d'abord que $A \in K^{n \times n}$ est diagonalisable.

Alors $\exists \{v_1, \dots\}$ une base composee de vecteurs propres de A .

Considerons

$$\begin{aligned} p(A) \cdot v_i &= a_0 v_i + a_1 A v_i + \dots \\ &= a_0 v_i + a_1 \lambda_i v_i + \dots \\ &= p(\lambda_i) v_i = 0 \end{aligned}$$

Supposons donc que A n'est pas diagonalisable.

Notons que

$$\text{Id} = \frac{\text{cof}(A - \lambda \text{Id})^T}{\det(A - \lambda \text{Id})} \cdot (A - \lambda \text{Id})$$

Alors

$$a_0 + a_1 \lambda \text{Id} + \dots = \text{cof}(A - \lambda \text{Id})^T \cdot (A - \lambda \text{Id})$$

$$\text{cof}(A - \lambda \text{Id})^T \cdot (A - \lambda \text{Id}) = B_0 A + \sum_{i=1}^{n-1} \lambda^i (B_i A - B_{i-1}) - \lambda_n B_{n-1}$$

Ce qui implique

$$\begin{aligned} a_0 \text{Id} &= B_0 A \\ a_i \text{Id} &= B_i A - B_{i-1} \text{ pour } i \in \{1, \dots, n-1\} \\ a_n \text{Id} &= -B_{n-1} \end{aligned}$$

On multiplie chacune de ces equations par A^i et on les additionne. On trouve alors

$$p(A) = 0 \quad \square$$

Definition 18 (Polynome minimal)

Le polynome unitaire de degre minimal parmi ceux, qui annullent la matrice $A \in K^{n \times n}$ est appele le polynome minimal de A .

Preuve

Ce polynome est unique.

Supposons qu'il existe q, p des polynomes qui annullent A . Alors

$$p \nmid q \text{ et } q \nmid p$$

Donc

$$p = qq' + r$$

ou $r \neq 0, \deg r < \deg p$, donc

$$0 = p(A) = r(A) + q'(A)q(A) = r(A)$$

Donc p n'est pas de degre minimal \nmid . \square

Corollaire 25

Soit $A \in K^{n \times n}$

- A^k est combinaison lineaire de $\text{Id}, A, \dots, A^{n-1}$ pour tout $k \in \mathbb{N}$
- A inversible, alors A^{-1} s'ecrit comme combinaison lineaire de $\text{Id}, A, \dots, A^{n-1}$

Preuve

— Pour $k \in 0, \dots, n-1$ clair.

Soit $k \geq n : x^k = q(x)p_A(x) + r(x)$, on evalue

$$A^k = q(A)p_A(A) + r(A) = r(A)$$

et r est de degre $n-1$.

—

$$\det A \neq 0 \quad \square$$

Donc il suffit de reformuler $p(A) = 0$.

4 Formes Bilineaires

Definition 19 (Forme Bilineaire)

— *BL1* $\forall u \in V,$

$$\begin{aligned} f_u : V &\rightarrow K \\ v &\rightarrow \langle u, v \rangle \end{aligned}$$

est lineaire

— *BL2* $\forall u \in V,$

$$\begin{aligned} f_u : V &\rightarrow K \\ v &\rightarrow \langle v, u \rangle \end{aligned}$$

est lineaire

La forme $\langle \cdot \rangle$ est dite symmetrique si pour tout $u, v \in V : \langle u, v \rangle = \langle v, u \rangle$.

La forme $\langle \cdot \rangle$ est dite non degeneratee a gauche (resp. a droite) si $\forall v \in V \langle v, w \rangle = 0 \Rightarrow w = 0$.

Soit V un espace vect de dimension n et $\{v_1, \dots, v_n\}$ une base.

$x, y \in V$ sont representes comme combinaison lineaire de $\{v_1, \dots\}$, soit $x = \sum x_i v_i$, et $y = \sum y_j v_j$, alors

$$\begin{aligned} \left\langle \sum x_i v_i, y \right\rangle &= \sum \langle x_i v_i, y \rangle \\ &= \sum x_i \langle v_i, y \rangle \\ &= \sum x_i \left\langle v_i, \sum y_j v_j \right\rangle \\ &= \sum x_i \sum y_j \langle v_i, v_j \rangle \\ &= (x_1, \dots, x_n) \begin{pmatrix} \langle v_1, v_1 \rangle & \dots & \langle v_1, v_n \rangle \\ \vdots & \ddots & \vdots \\ \langle v_n, v_1 \rangle & \dots & \langle v_n, v_n \rangle \end{pmatrix} (y_1, \dots, y_n)^T \end{aligned}$$

Proposition 26

Soit V un espace vectoriel sur K de dimension finie et $B = \{b_1, \dots, b_n\}$ une base de V .

Soit $f : V \times V \rightarrow K$ une forme bilineaire.

Les conditions suivantes sont equivalentes

- $rg(A_B^f) = n$
- f est non degeneratee a gauche
- f est non degeneratee a droite

Preuve

On demontre que 1 est equivalent a 2.

Il faut montrer que $\exists u \in V$ tel que $f(v, u) \neq 0$, or

$$f(v, u) = [v]_B^T \cdot A_B^f \cdot [u]_B$$

mais $\text{rg} A_B^f = n \Rightarrow [v]_B^T \cdot A_B^f \neq 0^T$.

Soit $i \in \{1, \dots, n\}$ tel que la i -eme composante de $([v]_B^T \cdot A_B^f)_i \neq 0$, alors pour $u = b_i$ on a fini.

Supposons maintenant que $\text{rg} A_B^f < n$, alors $\exists x \in K^n \setminus \{0\}$ tel que $x^T \cdot A_B^f = 0$ donc les lignes de A sont lineairements independantes. \square

4.1 Orthogonalite

Soit $\langle . \rangle$ une forme bilineaire symetrique.

Definition 20 (Orthogonalite)

Deux elements u, v sont orthogonaux si

$$\langle u, v \rangle = 0$$

Definition 21 (Complement orthogonal)

Soit $E \subseteq V$, alors

$$E^\perp = \{u \in V : u \perp e \forall e \in E\}$$

Proposition 27

Soit $E \subseteq V$, alors E^\perp est un sous-espace de V .

Lemme 28

Soit K un corps de caracteristique differente de 2.

Si $\langle u, u \rangle = 0$ pour tout $u \in V$, alors $\langle u, v \rangle = 0 \forall u, v \in V$

Preuve

Soient $u, v \in V$:

$$2 \langle u, v \rangle = \langle u + v, u + v \rangle - \langle u, u \rangle - \langle v, v \rangle \quad \square$$

et donc $\langle u, v \rangle = 0$.

Lecture 9: Formes bilineaires

Tue 23 Mar

Definition 22 (Matrices Congruentes)

Deux matrices $A, B \in K^{n \times n}$ sont congruentes s'il existe une matrice inversible $P \in K^{n \times n}$ inversible tel que

$$P^T \cdot A \cdot P = B$$

4.2 Orthogonalite

On supposera que $\langle \cdot, \cdot \rangle$ est une forme bilineaire symmetrique.

Definition 23 (Base orthogonale)

Soit $\{v_1, \dots, v_n\}$ une base de V . B est une base orthogonale si $\langle v_i, v_j \rangle = 0$ $\forall i \neq j$.

Lemme 29

Soit V de $\dim V = n$ et $B = \{v_1, \dots, v_n\}$ une base de V . B est orthogonale si et seulement si la matrice $A_B^{(\cdot, \cdot)}$ est une matrice diagonale.

Theorème 30

Soit $\text{char}(K) \neq 2$ et $\dim V = n < \infty$.

Alors V possede une base orthogonale.

Preuve

Dans le cas $n = 1$, le theoreme est trivial.

Si $n > 1$, alors on distingue deux cas.

Si $\langle u, u \rangle = 0$, la base est trivialement orthogonale.

Sinon, soit $u \in V$ tel que $\langle u, u \rangle \neq 0$.

On complete avec $v_2, \dots, v_n \in V$ tel que $\{u, v_2, \dots\}$ est une base de V .

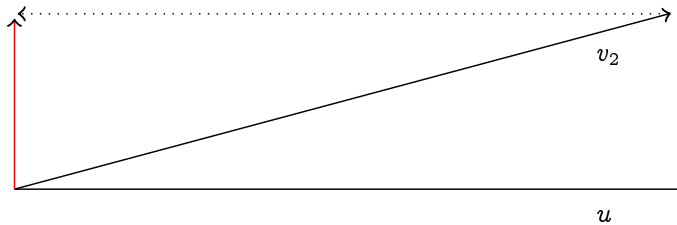


FIGURE 1 – gramschmidt

On construit une nouvelle base definie par

$$\{u, v_2 - \beta_2 u, \dots, v_n - \beta_n u\} := \{u, v'_2, \dots\}$$

Avec $\beta_i = \frac{\langle \vec{v}_i, u \rangle}{\langle u, u \rangle}$

On remarque que $u \perp v'_i$ et donc $u \perp \text{span}\{v'_2, \dots\}$.

Par hypothese de recurrence, on voit que qu'on peut repeter ce procede pour $\{v'_2, \dots, v'_n\}$

4.3 Matrices congruentes

On dit que $A \simeq B$ s'il existe $P \in K^{n \times n}$ inversible tel que

$$P^T A P = B$$

Etre congruent est une relation d'equivalence.

Lemme 31

Soit $B = \{v_1, \dots, v_n\}$ une base de V . V possede une base orthogonale si et seulement si $\exists D$ une matrice diagonale $\in K^{n \times n}$ tel que $A_B^{(\cdot)} \simeq D$

Algorithme pour trouver une matrice diagonale congruente a $A \in K^{n \times n}$ symmetrique

L'algorithme prend n iterations.

Apres la $i - 1$ ieme iteration A est transformee en

$$\begin{pmatrix} c_1 & & \\ & c_1 & \\ & & M \end{pmatrix}$$

Ou M est une matrice quelconque.

S'il existe un index $j \geq i$ tel que $b_{jj} \neq 0$, on echange la colonne i et la colonne j et la ligne i et la ligne j .

Si $b_{ij} = 0 \forall j \geq i$, on procede a la $i + 1$ -ieme iteration.

Pour chaque $j \in \{i + 1, \dots, n\}$ on additionne $\frac{-b_{ij}}{b_{ii}}$

Lecture 11: Formes Bilineaires definies positives et Espaces Euclidiens

Tue 30 Mar

4.4 Formes Bilineaires symmetriques definies positives

Ici, V sera toujours un espace vectoriel reel.

Definition 24 (Formes Bilineaires definies positives)

Une forme bilineaire $\langle \cdot \rangle$ est definie positive, si

$$\forall v \in V \setminus \{0\} : \langle v, v \rangle > 0$$

Une f.b.s. definie positive est appelee un produit scalaire.

Definition 25 (Norme d'un vecteur)

La longueur(ou norme) d'un vecteur de $v \in V$:

$$\|v\| = \sqrt{\langle v, v \rangle}$$

Definition 26

Un espace vectoriel reel muni d'un produit scalaire est appele espace euclidien.

Proposition 32

Pour $u \in V, \alpha \in \mathbb{R}$,

$$\|\alpha \cdot u\| = |\alpha| \|u\|$$

Preuve

$$\|\alpha \cdot u\| = \sqrt{\langle \alpha u, \alpha u \rangle} = |\alpha| \|u\|$$

□

Theorème 33 (Theoreme de Pythagore)

Pour $v, w \in V$: si $\langle v, w \rangle = 0$, alors

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2$$

Preuve

$$\begin{aligned} \|v + w\|^2 &= \langle v + w, v + w \rangle \\ &= \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle \\ &= \langle v, v \rangle + \langle w, w \rangle \end{aligned}$$

□

Proposition 34 (Regle du parallelogramme)

Pour $u, w \in V$:

$$\|u + w\|^2 + \|u - w\|^2 = 2\|u\|^2 + 2\|w\|^2$$

Sans preuve(facile)

Soit $w, v \in V$, on cherche α tel que

$$\langle v - \alpha w, w \rangle = 0$$

Donc

$$\alpha = \frac{\langle v, w \rangle}{\langle w, w \rangle}$$

On appelle α la composante de v sur w et αw la projection de v sur w .

Theorème 35 (Inegalite Cauchy-Schwarz)

Pour tout $v, w \in V$,

$$|\langle v, w \rangle| \leq \|v\| \|w\|$$

Preuve

On considere d'abord le cas special $\|w\| = 1$.

Donc, $\alpha = \langle v, w \rangle$, le theoreme de pythagore donne

$$\|v\|^2 = \|v - \alpha w\|^2 + \|\alpha \cdot w\|^2 \geq \alpha^2 \cdot \|w\|^2 = \alpha^2 = |\langle v, w \rangle|^2$$

Le cas general donne donc

$$\left\langle v, \|w\| \frac{w}{\|w\|} \right\rangle \leq \|w\|^2 \|v\| \quad \square$$

Theorème 36 (Inegalite triangulaire)

$$\|v + w\| \leq \|v\| + \|w\|$$

Preuve

$$\begin{aligned} \|v + w\|^2 &= \langle v + w, v + w \rangle^2 \\ &= \|v\|^2 + 2 \langle v, w \rangle + \|w\|^2 \\ &\leq (\|v\| + \|w\|)^2 \end{aligned} \quad \square$$

4.5 La methode de Gram Schmidt

Pour $\langle \cdot \rangle$ un produit scalaire, on a

$$\forall v \in V \setminus \{0\}, \langle v, v \rangle \neq 0$$

Lemme 37

soit V un espace euclidien et soient v_1, \dots, v_n deux-a-deux orthogonaux. Soit $v \in V$, il existe $a_1, \dots, a_n \in \mathbb{R}$ uniques tel que

$$v - a_1 v_1 - \dots - a_n v_n$$

est orthogonal a chaque v_i

Preuve

$$\left\langle v - \sum_{i=1}^n a_i v_i, v_j \right\rangle = \langle v, v_j \rangle - \left\langle \sum_{i=1}^n a_i v_i, v_j \right\rangle = \langle v, v_j \rangle - a_j \langle v_j, v_j \rangle \quad \square$$

On peut donc poser $a_j = \frac{\langle v, v_j \rangle}{\langle v_j, v_j \rangle}$

Le procede de Gram-Schmidt

Soit V un espace vectoriel euclidien et $\{v_1, \dots, v_n\}$.

Il existe un ensemble libre $\{u_1, \dots, u_n\}$ tel que

1. $\langle u_i, u_j \rangle = 0 \forall i \neq j$
2. $\forall k \in \{1, \dots, n\} :$

$$\text{span}\{v_1, \dots, v_k\} = \text{span}\{u_1, \dots, u_k\}$$

Pour ceci, on itere sur tous les elements de $\{v_1, \dots, v_n\}$, on pose

$$\begin{aligned} u_1 &= v_1 \\ u_2 &= v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} \cdot u_1 \\ &\vdots \\ u_3 &= v_3 - \frac{\langle v_3, u_1 \rangle}{\langle u_1, u_1 \rangle} \cdot u_1 - \frac{\langle v_3, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 \end{aligned}$$

etc.

Pour $i \in \{1, \dots, k\} :$

$$u_i = v_i - \sum_{j=1}^{i-1} \frac{\langle v_i, u_j \rangle}{\langle u_j, u_j \rangle} u_j$$

Par induction, on demontre que

$$\text{span}\{v_1, \dots, v_i\} = \text{span}\{u_1, \dots, u_{i-1}, v_i\}$$

Or u_i est combinaison lineaire des autres elements de la famille.

Corollaire 38

Soit $A \in \mathbb{R}^{m \times n}$ une matrice de rang-colonne plein.

On peut factoriser A comme

$$A = A' \cdot \begin{pmatrix} 1 & \dots & \mu_{ij} \\ \vdots & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Tel que A' est compose de colonnes 2-a-2 orthogonales pour le produit

scalaire standard.

Preuve

Pour a_i les colonnes de A , Gram-Schmidt donne

$$a'_i = a_i - \sum_{j=1}^{i-1} \frac{\langle a_i, a'_j \rangle}{\langle a'_j, a'_j \rangle} a'_j$$

Donc

$$a_i = \sum_{j=1}^{i-1} \frac{\langle a_i, a'_j \rangle}{\langle a'_j, a'_j \rangle} \cdot a'_j + a'_i \Rightarrow A = A' \cdot \begin{pmatrix} 1 & \dots & \mu_{ij} \\ \vdots & \ddots & \\ 0 & & 1 \end{pmatrix} \quad \square$$

Lecture 12: ...

Wed 31 Mar

Definition 27

Soit V un espace Euclidien, et $\langle \cdot \rangle$ un produit scalaire.

Une base $\{u_1, \dots, u_n\}$ orthogonale est appelee orthonormale si $\|u\|_i = 1 \forall i$.

Corollaire 39

Soit $V \in \mathbb{R}^{m \times n}$ une matrice de plein rang colonne, alors on peut factoriser $V = U^* \cdot R$ ou $U^* \in \mathbb{R}^{m \times n}$ dont les colonnes sont deux-a-deux orthogonales et de norme = 1, et ou R est une matrice triangulaire superieur

4.6 La methode des moindres carres

Soit $A \cdot x = b$ un systeme lineaire en m variables sans solution.

On cherche un x tel que $\|A \cdot x - b\|$ est minimale. On resout donc

$$\min_{x \in \mathbb{R}} \|A \cdot x - b\|$$

Theoreme 40

Soit V un espace euclidien et soient v_1, \dots, v_n des vecteurs deux-a-deux orthogonaux non-nuls. Soit $v \in V$ et $\alpha_i = \frac{\langle v, v_i \rangle}{\langle v_i, v_i \rangle}$, alors

$$\left\| v - \sum_{i=1}^n \alpha_i v_i \right\| \leq \left\| v - \sum_{i=1}^n \beta_i v_i \right\|$$

pour tout $\beta_1, \dots, \beta_n \in \mathbb{R}$

Preuve

on a

$$\begin{aligned} \left\| v - \sum_{i=1}^n \beta_i v_i \right\|^2 &= \left\| \underbrace{v - \sum_{i=1}^n \alpha_i v_i}_{\text{perpendiculaire à tous les } v_i} - \sum_{i=1}^n (\beta_i - \alpha_i) v_i \right\|^2 \\ &= \left\| v - \sum_{i=1}^n \alpha_i v_i \right\|^2 + \left\| \sum_{i=1}^n (\beta_i - \alpha_i) v_i \right\|^2 \geq \left\| v - \sum_{i=1}^n \alpha_i v_i \right\|^2 \quad \square \end{aligned}$$

Donc, pour résoudre $\min_{x \in \mathbb{R}^n} \|Ax - b\|$, on calcule d'abord une base orthogonale de l'espace engendré par les vecteurs-collonne de A .

Ensuite, on calcule la projection de b , c'est-à-dire $\sum_{i=1}^n \frac{\langle b, a_i^* \rangle}{\langle a_i^*, a_i^* \rangle} a_i^*$.

Ensuite, on résout $Ax = \text{proj}(b)$ et on trouve un x proche.

Theorème 41

Les solutions du système

$$A^T \cdot Ax = A^T b$$

sont les solutions optimales de $\min_{x \in \mathbb{R}^n} \|Ax - b\|$

Preuve

x est une solution optimale $\iff Ax = \text{proj}(b)$, de plus $\text{proj}(b)$ est le vecteur v unique dans $\{A \cdot x : x \in \mathbb{R}^n\}$ tel que $b - v \perp \text{span}\{A\} = \{A \cdot x : x \in \mathbb{R}^n\}$

Donc

$$A^T Ax = A^T b \iff A^T (Ax - b) = 0 \iff Ax - b \perp \{A \cdot x : x \in \mathbb{R}^n\} \quad \square$$

4.7 Formes sesquilineaires et produits hermitiens

Soit $v = \begin{pmatrix} a_1 + ib_1 \\ \vdots \\ a_n + ib_n \end{pmatrix} \in \mathbb{C}^n$, avec $a_i, b_i \in \mathbb{R}$.

On définit

$$\sum_{i=1}^n a_i^2 + b_i^2 = \sum_{i=1}^n v_i \overline{v_i}$$

Definition 28 (Produit Hermitien)

Soit V un espace vectoriel sur \mathbb{C} , $\langle \cdot, \cdot \rangle$ une application, alors on a

- PH1 : $\langle v, w \rangle = \overline{\langle w, v \rangle} \forall v, w \in V$
- PH2

$$\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle, \langle w + u, v \rangle = \langle v, w \rangle + \langle u, w \rangle$$

— PH3

$$\forall x \in \mathbb{C}, u, v \in V, \langle xu, v \rangle = x \langle u, v \rangle, \langle u, xv \rangle = \bar{x} \langle u, v \rangle$$

1. Une forme sesquilineaire satisfait PH2, PH3
2. Forme hermitienne satisfait PH1, PH2, PH3
3. Un produit hermitien satisfait PH1, PH2, PH3 et de plus

$$\langle v, v \rangle > 0 \forall v \in V \setminus \{0\}$$

Le produit hermitien est l'analogue d'un produit scalaire.

Definition 29 (Matrice hermitienne)

$A \in \mathbb{C}^{n \times n}$ est appelée hermitienne si $A^T = \bar{A}$

Proposition 42

Soit V un espace vectoriel sur \mathbb{C} de dimension finie et soit B une base de V . Une forme sesquilineaire est une forme hermitienne si et seulement si A_B^f est une matrice hermitienne.

Si B, B' sont deux bases différentes, alors $f(v, w) = [v]_B^T A_B^f \overline{[w]_B}$.

Si B' est une autre base, et $P_{BB'}, P_{B'B}$ les matrices de changement de base correspondantes. Alors on a

$$[v_{B'}]^T (P_{B'B})^T A_B^f \overline{P_{B'B} [w]_B} = f(v, w)$$

On en déduit que

$$A_{B'}^f = (P_{B'B})^T A_B^f \overline{P_{B'B}}$$

Definition 30 (Matrices Complexes congruentes)

Deux matrices complexes A, B sont congruentes complexes, si il existe P une matrice inversible satisfaisant

$$A = P^T B \bar{P}$$

Comme avant, une base $B = \{b_1, \dots\}$ est une base orthogonale si et seulement si $A_B^{\langle \cdot, \cdot \rangle}$ est diagonale.

Theorème 43

Soit V un espace vectoriel complexe et $\langle \cdot, \cdot \rangle$ une forme hermitienne, alors V possède une base orthogonale.

On utilise le procédé analogue aux espaces hermitiens.

Lecture 13: Matrices Symmetriques

Tue 13 Apr

Theorème 44 (Theoreme Spectral)

Soit $A \in \mathbb{R}^{n \times n}$ symmetrique, alors il existe $P \in \mathbb{R}^{n \times n}$ orthogonale tel que

$$P^T \cdot A \cdot P$$

est diagonale.

Donc A est congruent a une matrice diagonale et est semblable D .

Lemme 45

Soit $A \in \mathbb{C}^{n \times n}$ une matrice hermitienne, alors toutes ses valeurs propres sont reelles.

Preuve

Soit $\lambda \in \mathbb{C}$ une valeur propre et $v \in \mathbb{C}^n \setminus \{0\}$ un vecteur propre associe a λ .
On va montrer que $\lambda v^T \bar{v} = \bar{\lambda} v$.

On a

$$\lambda v^T \bar{v} = v^T A^T \bar{v} = v^T \bar{A} \bar{v} = v^T \bar{\lambda} \bar{v} = \bar{\lambda} v \bar{v} \quad \square$$

Corollaire 46

Soit $A \in \mathbb{R}^{n \times n}$ resp. $\mathbb{C}^{n \times n}$ une matrice symmetrique resp., hermitienne. Alors A possede une valeur propre reelle.

Preuve

Les valeurs propres de A sont les racines reelles resp. complexes du polynome caracteristique de A .

Soit $\lambda \in \mathbb{C}$ une racine, donc λ est une valeur propre de A sur \mathbb{C}^n , par le lemme ci-dessus, λ est reel.

Et donc λ est une valeur propre d'une matrice reelle de A . \square

Prouvons maintenant le theoreme spectral.

Preuve

On demontre le cas reel.

Soit $A \in \mathbb{R}^{n \times n}$ symmetrique. Il existe $U \in \mathbb{R}^{n \times n}$ orthogonale tel que $U^T A U$ est orthogonale.

On procede par recurrence.

Le cas $n = 1$, $A = (a_{11})$ est clair.

Pour $n > 1$, soit $\lambda \in \mathbb{R}$ une valeur propre de A et $v \in \mathbb{R}^n \setminus \{0\}$ un vecteur propre associe tel que $v^T v = 1$.

Soit $\{v_1, u_2, \dots\}$ une base de \mathbb{R}^n .

Avec Gram-Schmidt, on peut supposer que cette base est orthonormale.

Soit U la matrice donnee par les colonnes $(u_2, \dots, u_n) \in \mathbb{R}^{n \times (n-1)}$, on considere U

${}^T AU \in \mathbb{R}^{(n-1) \times (n-1)}$, c'est une matrice symétrique (parce que A est symétrique).

Par récurrence, il existe une matrice orthogonale tel que $K^T U^T A U K$ est diagonale et réelle.

Posons $P = (v, U \cdot K) \in \mathbb{R}^{n \times n}$.

P est orthogonale, en effet

$$P^T P = \begin{pmatrix} v^T \\ K^T U^T \end{pmatrix} \begin{pmatrix} v \\ U K \end{pmatrix} = \begin{pmatrix} v^T v & v^T U K \\ K^T U^T v & K^T U^T U K \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \text{Id} \end{pmatrix}$$

Et donc

$$P^T A P = \begin{pmatrix} v^T \\ K^T U^T \end{pmatrix} A(V, U K) \quad \square$$

Or v est orthogonal a tous les u_i et donc cette matrice est orthogonale.