Algebre Lineaire II

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Introduction

Tue 23 Feb

1 Polynomes

Definition 1 (Centre d'un anneau)
Le centre $Z(R)$ est l'ensemble des elements x satisfaisant

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

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 $a_0 + \ldots + a_n x^n = 0$ 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

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

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

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

Donc $R[X]$ est stable pour $+, \cdot$ et donc immediatement 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 $m+n$-ieme coefficient de $f(x)g(x)$ est $a_n b_m$ et donc si R est integre,$R[x]$ l'est aussi. □

Definition 5 (Degre d'un polynome)
Soit $f(x) = a_0 + \ldots \in R[X]$, $f(x) \neq 0$. On definit

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

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

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

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 $f(x) = a_0 + \ldots, g(x) = b_0 + \ldots$,$\deg f = n, \deg g = m$. Le $n+m$ ieme coefficient de $f \cdot g = a_n \cdot b_m \neq 0$ □

Soit $p(x) \in R[x]$, ce polynome induit une application $f_p : R \to R$, on ecrit aussi $p(r)$

> **Theorème 4**
> *Soit K un corps et $r_0, r_1, \ldots, r_n \in K$ des elements distincts et soient $g_0, \ldots, g_n \in K$.*
> *Il existe un seul polynome $f \in K[x]$ tel que*
>
> 1. $\deg f \leq n$
> 2. $f(r_i) = g_i$

Preuve
On cherche $a_0, \ldots a_n$ tel que

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

Donc, on cherche

$$\begin{pmatrix} 1 & r_0 & \ldots & r_0^n \\ \vdots & \ldots & \ldots & \ldots \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \end{pmatrix} = \begin{pmatrix} g_1 \\ \ldots \\ \ldots \end{pmatrix}$$

Il faut donc montrer que la matrice ci-dessus a un determinant non nul.
On le montre par induction sur n.
Dans le cas $n = 0$, le determinant 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 characteristique 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 egaux si et seulement si leurs evaluations sont les memes.

Preuve
Une direction est triviale.
L'autre suit immediatement du theoreme 1.6 $\square$

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 $\deg f \geq g$, 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

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

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 $(x - a)|f(x)$*

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 $f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r = 0$ et donc $(x - a)|f(x)$ $\square$

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 montre 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 $\deg d$. $\lightning$ $\square$

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

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

- *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 dependance lineaire 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 elements irreductibles

Un polynome $p(x)$ est irreductible si le degre 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

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

Est-ce que cette factorisation est unique ?

Theorème 14
Soit $p(x) \in K[x] \setminus \{0\}$ irreductible et supposons que $p|f_1(x) \ldots f_k(x)$, alors il existe i tel que $p(x)|f_i(x)$

Preuve
Par recurrence, il suffit de demontrer l'assertion pour $k = 2$.
Supposons que $p|f \cdot g$, $f, g \in K[x] \setminus \{0\}$.
Si $p \not| f$, alors $\gcd(p, f) = 1$. Donc, il existe $u, v \in K[x]$ tel que $up + vf = 1$, donc on a

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

Theorème 15 (La factorisation est unique)
La factorisation est unique a l'ordre pres des p_i.

Preuve
Soit $f(x) = a \prod p_i(x)$ et $f(x) = a \prod q_j(x)$ une autre factorisation en elements irreductible.
Par recurrence sur k.
Si $k = 1$, alors

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

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

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

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

$$p_2(x) \ldots = q_1(x) \ldots q_l(x) \qquad \square$$

Par recurrence, cette factorisation existe et est la meme a ordre pres.

Corollaire 16
Soit $f(x) \in K[x] \setminus \{0\}$ *et* $\alpha_1 \dots$ *des racines de* f *de multiplicite* $k_1, \dots, k_l$ *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 a 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 a* 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 associe a 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 associe a* λ_i.
Dans l'autre sens, les arguments sont similaires. □

Definition 14
Un endomorphisme f *sur un espace vectoriel de dimension finie est appele diagonalisable s'il existe une base tel que* $\{v_1, \dots\}$ *de* V *composee de vecteurs propres.*

Lecture 5: Vecteurs/Valeurs Propres

Tue 09 Mar

Corollaire 18
*Soit $f : V \to V$ 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 $f : V \to V$ un endomorphisme et λ une valeur propre de f, alors

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

est l'espace propre de f associe a λ.
$\dim E_\lambda$ *est la multiplicite geometrique de λ.*

Lemme 19
*Soit $f : V \to V$ 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

$$0 = \alpha_1 f(v_1) + \alpha_2 f(v_2)$$
$$0 = \alpha_1 \frac{\lambda_1}{\lambda_2} v_1 + \alpha_2 v_2$$
$$0 = \alpha_1 (1 - \frac{\lambda_1}{\lambda_2}) v_2$$

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

sont lin. dependants.. Soit

$$\alpha_1 v_1 + \ldots = 0$$

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

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

En soustrayant les deux egalites, on trouve

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

□

Ce qui contredit la minimalite.

Corollaire 20
Soit $f : V \to V$ *un endomorphisme de* V *sur* K *et* $\dim V = n$*.*
Soient $\lambda_1, \ldots,$ *les valeurs propres differentes de* f*.*
Soit $n_1 \ldots$ *les multiplicites geometriques respectives.*
Soient $B_i = \left\{ v_1^{(i)}, \ldots, v_{n_i}^{(i)} \right\}$ *des bases de* E_{λ_i}*, alors*

$$\bigcup_i B_i$$

est un ensemble libre.
f *est diagonalisable* $\iff$ $n_1 + \ldots + n_r = n$

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* $\sum n_i = n$*.*

Lecture 7: Polynome caracteristique

Wed 10 Mar

3 Le polynome caracteristique

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

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

On observe que λ est une valeur propre de f si et seulement si λ est une racine de p_A.
Soit $f : V \to V$ un endomorphisme, $B = \{v_1, \ldots\}$ une base de V. Le polynome caracteristique de f est donne par

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

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

Definition 17 (Multiplicite algebrique)
La multiplicite algebrique d'une valeur propre est la multiplicite comme racine du polynome caracteristique.

Proposition 21
Soit f un endomorphisme de $V \to V$.
Soit $\lambda \in K$ une valeur propre.
La multiplicite geometrique de λ est au plus la mutliplicite algebrique.

Preuve
Soit $\{v_1, \ldots, v_r\}$ une base de E_λ, on complete cette base en une base de V avec $\{w_1, \ldots, w_{n-r}\}$. Dans cette base, la representation de la matrice de $A - \lambda \operatorname{Id}$ implique que

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

et donc r est au plus la multiplicite algebrique.

Theorème 22 (Theoreme de diagonalisation)
Soit V un espace vectoriel sur K de dimension n, $f : V \to V$ un endomorphisme $\lambda_1, \ldots \in K$ 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* $B = \{v_1, \ldots\}$ *une base composee de vecteurs propres.* A_B *est une matrice diagonale, alors* $p_f(x) = \det(A_B - x\,\mathrm{Id}) = (-1)^n \prod(\lambda_i - x)^{g_i}$.
De plus $\dim(\ker(A_B - \lambda_i\,\mathrm{Id})) = g_i$

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

Theorème 23 (Evaluation d'une matrice dans un polynome)
Soit $p(x) = a_0 + \ldots + a_n x^n \in K[x]$ *Pour* $A \in K^{n\times n}$, *on definit*

$$p(A) = a_0\,\mathrm{Id} + \ldots + a_n A^n$$

Theorème 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 $\exists\{v_1, \ldots\}$ *une base composee de vecteurs propres de* A.
Considerons

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

Supposons donc que A *n'est pas diagonalisable.*
Notons que

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

Alors

$$a_0 + a_1\lambda\,\mathrm{Id} + \ldots = cof(A - \lambda\,\mathrm{Id})^T \cdot (A - \lambda\,\mathrm{Id})$$

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

Ce qui implique

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

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

$$p(A) = 0$$

□

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

$$p \not| q \text{ et } q \not| p$$

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 $\lightning$. □

Corollaire 25
Soit $A \in K^{n\times n}$
- *A^k est combinaison lineaire de $\operatorname{Id}, A, \dots, A^{n-1}$ pour tout $k \in \mathbb{N}$*
- *A inversible, alors A^{-1} s'ecrit comme combinaison lineaire de $\operatorname{Id}, A, \dots, A^{n-1}$*

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 $n-1$.
- $$\det A \neq 0$$

  □

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

Lecture 8: Formes bilineaires

Wed 17 Mar

4 Formes Bilineaires

Definition 19 (Forme Bilineaire)

— *BL1* $\forall u \in V$,

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

est lineaire

— *BL2* $\forall u \in V$,

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

est lineaire

La forme $\langle . \rangle$ est dite symmetrique si pour tout $u, v \in V : \langle u, v \rangle = \langle v, u \rangle$.
La forme $\langle . \rangle$ est dite non degeneree 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 $\{v_1, \ldots, v_n\}$ une base.
$x, y \in V$ sont representes comme combinaison lineaire de $\{v_1, \ldots\}$, soit $x = \sum x_i v_i$, et $y = \sum y_i v_i$, alors

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

Proposition 26
Soit V un espace vectoriel sur K de dimension finie et $B = \{b_1, \ldots, b_n\}$ une base de V.
Soit $f : V \times V \to K$ une forme bilineaire.
Les conditions suivantes sont equivalentes

— $rg(A_B^f) = n$
— *f est non degeneree a gauche*
— *f est non degeneree 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 $rgA_B^f = n \Rightarrow [v]_B^T \cdot A_B^f \neq 0^T$.
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 $rgA_B^f < n$*, 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.* □

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 characteristique 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 $u, v \in V$ *:*

$$2 \langle u, v \rangle = \langle u + v, u + v \rangle - \langle u, u \rangle - \langle v, v \rangle$$ □

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 $\langle . \rangle$ est une forme bilineaire symmetrique.

Definition 23 (Base orthogonale)
Soit $\{v_1, \ldots, v_n\}$ *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* $B = \{v_1, \ldots, v_n\}$ *une base de* V. B *est orthogonale si et seulement si la matrice* $A_B^{\langle . \rangle}$ *est une matrice diagonale.*

Theorème 30
Soit $char(K) \neq 2$ *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 $v_2, \ldots, v_n \in V$ *tel que* $\{u, v_2, \ldots\}$ *est une base de* V.

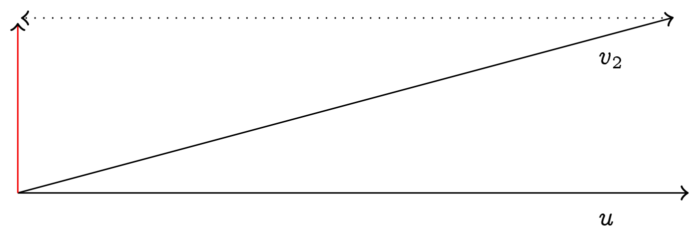

FIGURE 1 – gramschmidt

On construit une nouvelle base definie par

$$\{u, v_2 - \beta_2 u, \ldots, v_n - \beta_n u\} := \{u, v_2', \ldots\}$$

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

On remarque que $u \perp v_i'$ et donc $u \perp span\{v_2', \ldots\}$.
Par hypothese de recurrence, on voit que qu'on peut repeter ce procede pour $\{v_2', \ldots, v_n'\}$

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 $B = \{v_1, \ldots, v_n\}$ 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 $A_B^{\langle . \rangle} \simeq D$

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 $j \in \{i+1, \ldots, n\}$ 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 $\langle . \rangle$ est definie positive, si

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

Une f.b.s. definie positive est appellee 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

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

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

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

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

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

□

Theorème 36 (Inegalite triangulaire)

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

Preuve

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

□

4.5 La methode de Gram Schmidt

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

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

Lemme 37
soit V un espace euclidient et soient $v_1, \ldots, v_n$ deux-a-deux orthogonaux. Soit $v \in V$, il existe $a_1, \ldots, a_n \in \mathbb{R}$ uniques tel que

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

est orthogonal a chaque v_i

Preuve

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

□

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 $\{v_1, \ldots, v_n\}$.
Il existe un ensemble libre $\{u_1, \ldots, u_n\}$ tel que

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

$$span\,\{v_1, \ldots, v_k\} = span\,\{u_1, \ldots, u_k\}$$

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

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

etc.
Pour $i \in \{1, \ldots, k\}$:

$$u_1 = v_i - \sum_{j=1}^{i-1} \frac{\langle v_i, u_j \rangle}{\langle u_j, u_j \rangle} u_j$$

Par induction, on demontre que

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

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*

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

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

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

Lecture 12: ...

Wed 31 Mar

Definition 27

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

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

Theorème 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

$$\left\| v - \sum_{i=1}^{n} \beta_i v_i \right\|^2 = \left\| \underbrace{v - \sum_{i=1}^{n} \alpha_i v_i}_{\text{perpendiculaire a tous les } v_i} - \sum_{i=1}^{n} (\beta_i - \alpha_i) v_i \right\|^2$$

$$= \left\| v - \sum_{i=1}^{n} \alpha_i v_i \right\|^2 + \left\| \sum_{i=1}^{n} (\beta_i - \alpha_i) v_i \right\|^2 \geq \left\| v - \sum_{i=1}^{n} \alpha_i v_i \right\| \qquad \square$$

Donc, pour resourdre $\min_{x \in \mathbb{R}^n} ||Ax - b||$, on calcule d'abord une base orthogonale de l'espace engendre par les vecteurs-collone de A.
Ensuite, on calcule la projection de b, cad $\sum_{i=1}^{n} \frac{\langle b, a_i^* \rangle}{\langle a_i^*, a_i^* \rangle}$.
Ensuite, on resout $Ax = proj(b)$ et on trouve un x proche.

Theorème 41
Les solutions du systeme

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

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

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

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

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 definit

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

Definition 28 (Produit Hermitien)
Soit V un espace vectoriel sur $\mathbb{C}$, $\langle . \rangle$ 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*

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

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 hermition est l'analogue d'un produit scalaire.

Definition 29 (Matrice hermitienne)
$A \in \mathbb{C}^{n\times n}$ *est appellee hermitienne si* $A^T = \overline{A}$

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 differentes, 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 correspondentes. Alors on a

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

On en deduit 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*

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

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

Theorème 43
Soit V *un espace vectoriel complexe et* $\langle . \rangle$ *une forme hermitienne, alors* V *possede une base orthogonale.*

On utilise le procede 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 $\lambda v^T \overline{v} = \overline{\lambda} v$.
On a
$$\lambda v^T \overline{v} = v^T A^T \overline{v} = v^T \overline{A v} = v^T \overline{\lambda} \overline{v} = \overline{\lambda} v \overline{v} \qquad \square$$

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 relles resp. complexes du polynome characteristique 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 $\{v_1, u_2, \ldots\}$ 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 $(u_2, \ldots, u_n) \in \mathbb{R}^{n\times(n-1)}$, on considere U

${}^T AU \in \mathbb{R}^{(n-1)\times(n-1)}$, *c'est une matrice symmetrique (parce que A est symmetrique).*
Par recurrence, il existe une matrice orthogonale tel que $K^T U^T AUK$ est diagonale et reelle.
Posons $P = (v, U \cdot K) \in \mathbb{R}^{n\times n}$.
P est orthogonale, en effet

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

Et donc

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

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

Lecture 14: Formes quadratiques reelles

Wed 14 Apr

5 Formes quadratiques reelles et matrices symmetriques reelles

Definition 31 (Sphere)
$S^{n-1} \subseteq \mathbb{R}^n$ est defini comme $S^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\}$

Definition 32 (Forme Quadratique)
Une forme quadratique est une application $f : \mathbb{R}^n \to \mathbb{R}, x \to x^T Ax$, avec A une matrice symmetrique [1]

Probleme d'optimisation

On veut trouver le maximum

$$\max_{x \in S^{n-1}} x^T Ax$$

L'existence du maximum est garantie car S^{n-1} est compacte et $x \to x^T Ax$ est continue.
Donc il existe $x \in S^{n-1} : x^T Ax \geq y^T Ay \forall y \in S^{n-1}$.
Par symmetrie, il existe au moins deux solutions optimales sur S^{n-1}.

Lemme 47
Soit $A \in \mathbb{R}^{n\times n}$ symmetrique et $v \in S^{n-1}$ une solution optimale. On a

$$Av = \lambda v$$

1. La symmetrie n'est pas necessaire, car $x^T Bx = x^T(\frac{1}{2}B + \frac{1}{2}B^T)x$

pour $\lambda \in \mathbb{R}$ cad A possede une valeur propre reelle.

Preuve

On suppose que $A \cdot v \neq \lambda v \forall \lambda \in \mathbb{R}$ (avec v une solution optimale du systeme).

$$A \cdot v = \alpha v + \beta w (\alpha, \beta \in \mathbb{R})$$

Notons que

$$\sqrt{(1-x^2)}v + xw, x \in [-1,1] \in S^{n-1}$$

Posons

$$g(x) := (\sqrt{1-x^2}v + xw)^T A(\sqrt{1-x^2}v + xw)$$

avec $g(0) = v^T Av$, il reste a montrer que $g'(0) \neq 0$.
On a

$$\begin{aligned} g(x) &= (1-x^2)v^T Av + \sqrt{1-x^2}xv^T Aw + x\sqrt{1-x^2}w^T Av + x^2 w^T Aw \\ &= (1-x^2)v^T Av + 2x\sqrt{1-x^2}v^T Av + x^2 w^T Aw \end{aligned}$$

Donc

$$g'(0) = 2w^T Aw = 2\beta \neq 0$$

□

Definition 33 (Matrice Symmetrique definie positive/negative)
Soit $A \in \mathbb{R}^{n \times n}$ symmetrique, A est

- *definie positive si $x^T Ax > 0 \forall x \in \mathbb{R}^n \setminus \{0\}$*
- *definie negative si $x^T Ax < 0 \forall x \in \mathbb{R}^n \setminus \{0\}$*
- *semi-definie positive si $x^T Ax \geq 0 \forall x \in \mathbb{R}^n$*
- *semi-definie negative si $x^T Ax \leq 0 \forall x \in \mathbb{R}^n$*

Theorème 48
Une matrice symmetrique $A \in \mathbb{R}^{n \times n}$ est

- *definie positive si et seulement si toutes ses valeurs propres sont > 0*
- *definie negative si et seulement si toutes ses valeurs propres sont < 0*
- *semi-definie positive si et seulement si toutes ses valeurs propres sont ≥ 0*
- *semi-definie negative si et seulement si toutes ses valeurs propres sont ≤ 0*

Preuve

$$A = P \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} P^T$$

— *Si* $\lambda_1, \dots, \lambda_n > 0$*, alors, en reecrivant* $v = \sum \beta_i p^i$

$$v^T A v = \sum_{i=1}^{n} \beta_i^2 \lambda_i > 0$$

□

On en deduit facilement les autres points.

Definition 34 (k-mineur principal)
Soit $A \in K^{n \times n}$*. On considere la matrice formee par les* k *premieres lignes et colonnes de* A*, notons la* B*, le* k*-mineur principal est le determinant de* B*.*

Theorème 49
Soit $A \in \mathbb{R}^{n \times n}$ *une matrice symmetrique.*
A est definie positive si et seulement si tous ses mineurs principaux sont strictement positif.

Preuve
Si A est definie positive, alors C_k *est definie positive (ie. toutes les sous-matrices). On a*

$$C_k = P_k \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_k \end{pmatrix} P_k^T$$

Ou on a utilise la decomposition selon le theoreme spectral.
Par le theoreme ci-dessus $\det C_k > 0$
Montrons l'implication inverse.
Supposons maintenant que le determinant $\det(C_k) > 0 \forall k \in \{1, \dots, n\}$*.*
On veut montrer que $x^T A x > 0 \forall x \in \mathbb{R}^n \setminus \{0\}$*.*
On applique l'algorithme d'orthogonalisation sur A*.*
Par recurrence, on a jamais echange de lignes et de colonnes car sinon un determinant serait nul.
L'algorithme produit une matrice triangulaire superieure $R \in \mathbb{R}^{n \times n}$ *(avec une diagonale contenant des* 1*) tel que*

$$R^T A R = \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_n \end{pmatrix}$$

□

On observe donc que $\det C_k = c_1 \dots c_k$ *et donc tous les* c_i *sont positifs.*