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

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

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 $(x - a)|f(x)$ □

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 $\deg d$. ↯ □

Definition 10 (Polynome Unitraire)
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 $p|f_1(x) \dots f_k(x)$, 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

$$upg + vfg = g \Rightarrow p|upg + vfg \Rightarrow p|g$$ □

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

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

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

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

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

$$p_2(x) \dots = q_1(x) \dots q_l(x)$$ □

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 $\{v_1, \ldots, v_n\}$ 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 $\iff$ $\exists B' = \{w_1, \ldots\}$ 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 $v_1, \ldots, v_r$ des vecteurs propres associes aux valeurs propres $\lambda_1, \ldots, \lambda_r$ distinctes.
Alors $\{v_1, \ldots, v_r\}$ 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

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

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

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

□

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 $p_f(x) = \det(A_B - x \operatorname{Id}) = (-1)^n \prod (\lambda_i - x)^{g_i}$. De plus $\dim(\ker(A_B - \lambda_i \operatorname{Id})) = g_i$

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*

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

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

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

Alors

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

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

Ce qui implique

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

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

$$p(A) = 0$$

□

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

Preuve
- *Pour $k \in 0, \ldots, n-1$ 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 $i \in \{1, \ldots, n\}$ 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 $u, v \in V$:

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

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 $\langle . \rangle$ 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 $A_B^{\langle\cdot\rangle}$ 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.

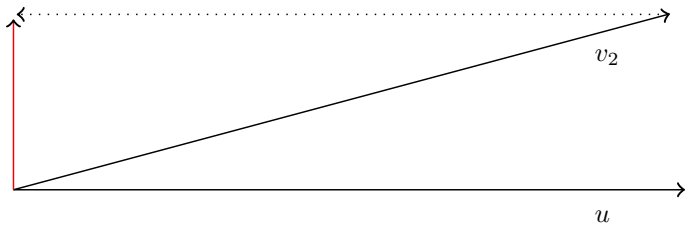

FIGURE 1 – gramschmidt

On construit une nouvelle base definie par

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

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

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

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

Lecture 12: ...

Wed 31 Mar

Definition 27

Soit V un espace Euclidien, et $\langle . \rangle$ un produit scalaire.
Une base $\{u_1, \ldots, u_n\}$ 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 $v_1, \ldots, v_n$ 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 $\beta_1, \ldots, \beta_n \in \mathbb{R}$

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

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

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

$$\lambda v^T \overline{v} = v^T A^T \overline{v} = v^T \overline{A} \overline{v} = v^T \overline{\lambda} \overline{v} = \overline{\lambda} v \overline{v} \qquad \square$$

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 $U^T AU$ 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

$$Av = \lambda v$$

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

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

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

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

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

□

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 $x^T Ax > 0 \forall x \in \mathbb{R}^n \setminus \{0\}$.
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

$$R^T AR = \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_n \end{pmatrix} \qquad \square$$

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

Lecture 15: Theoreme Spectral

Tue 20 Apr

Theorème 50 (Theoreme spectral reel)
Soit $A \in \mathbb{R}^{n\times n}$ symmetrique cad $A^T = A$, alors il existe $P \in \mathbb{R}^{n\times n}$ orthogonale tel que

$$A = PDP^T$$

Avec D une matrice diagonale.
Donc A est semblable et congruente a une matrice diagonale. Pour $P = (P_1, P_2, \dots)$ les vecteurs colonne de P, $P_1, \dots$ forment une base orthonor-

male de vecteurs propres de A, cad

$$\begin{aligned} A \cdot p_i &= PDP^T P_i \\ &= P\lambda_i e_i = \lambda_i P e_i \end{aligned}$$

Definition 35
Soit $K \subseteq \{1, \ldots, n\}$ *et* $A \in \mathbb{R}^{n \times n}$*, ecrivons*

$$K = \{l_1, \ldots, l_k\} \text{ ou } l_1 < l_2 < \ldots < l_k$$

Alors $A_k \in \mathbb{R}^{k \times k}$*, avec* $a_{k,ij} = a_{l_i, l_j}$.

Theorème 51
Soit $A \in \mathbb{R}^{n \times n}$ *symmetrique.*
A est semi definie positive si

Preuve
Soit $A \in \mathbb{R}^{n \times n}$ *symmetrique et semi definie positive pour* $K \subseteq \{l_1, \ldots\}$.
A_k *est semi-definie positive, donc*

$$A_K = P^{K^T} D'_k P_K$$

Et donc

$$\det(A_k) > 0$$ □

L'autre implication est identique au theoreme spectral.

Theorème 52
Soit $A \in \mathbb{R}^{n \times n}$ *symmetrique et soit* $f : \mathbb{R}^n \to \mathbb{R}$ *definie par*

$$f(x) = x^T A x$$

, alors

$$\max_{x \in S^{n-1}} f(x) = \lambda_1$$

et

$$\min_{x \in S^{n-1}} f(x) = \lambda_n$$

sont des valeurs propres qui satisfont

$$\lambda_1 > \lambda_2 > \ldots > \lambda_n$$

Preuve
Si $P = (p_1, \ldots, p_n)$ *alors* $\{p_1, \ldots\}$ *est une base orthonormale de vecteurs propres de A.*
Soit $x \in \mathbb{R}^n$ *et* $\|x\|_2^2 = x^T x$ *On peut donc reecrire*

$$x^T x = \sum_{i=1}^{n} (\alpha_i)^2$$

Donc, pour $x \in S^{n-1}$, on a

$$\begin{aligned} f(x) &= x^T \sum \beta_i \lambda_i p_i \\ &= \sum_{i=1}^{n} \beta_i^2 \lambda_i \end{aligned}$$

□

Theorème 53 (Theoreme Min-Max)
Soit $A \in \mathbb{R}^{n\times n}$ symmetrique et $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ les valeurs propres de A. Alors

$$\begin{aligned} \lambda_k &= \max_{U\leq\mathbb{R}^n, \dim(U)=k} \min_{x\in S^{n-1}\cap U} x^T A x \\ &= \min_{U\leq\mathbb{R}^n, \dim(U)=n-k} \max_{x\in S^{n-1}\cap U} x^T A x \end{aligned}$$

Preuve
λ_k est atteint par l'espace span $\{p_1, \ldots, p_k\}$ et $p_k^T A p_k = \lambda_k$. Pour

$$x = \sum_{i=1}^{k} \alpha_i p_i \in span\{p_1, \ldots, p_k\} \cap S^{n-1}$$

Alors

$$x^T A x = \sum_{i=1}^{k} \alpha_i^2 \lambda_i \geq \lambda_k$$

Donc

$$\min_{x\in S^{n-1}, x\in span\{p_1,\ldots,p_k\}}$$

Il reste a montrer que pour tout $U \subseteq \mathbb{R}^n$, on a

$$\dim(U) = k \Rightarrow \min_{x\in S^{n-1}, x\in U} x^T A x \leq \lambda_k$$

□

Lecture 16: Valeurs Singulieres

Wed 21 Apr

5.1 Decomposition en valeurs singulieres

Theorème 54 (Decomposition en valeurs singulieres)
Soit $A \in \mathbb{C}^{m\times n}$, il existe des matrices unitaires $P \in \mathbb{C}^{m\times n}, Q \in \mathbb{C}^{n\times n}$ tel que $A = PDQ$ avec $D \in \mathbb{R}_{\geq 0}^{m\times n}$ une matrice diagonale.

Preuve
On veut $A = P \begin{pmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_r \end{pmatrix} Q$ *avec $\sigma_1 \geq \ldots \geq \sigma_r > 0$ les valeurs singulieres.*
Soit $u_1, \ldots, u_n$ une base orthogonale par rapport au produit hermitien standard

compose de valeurs propres associees a $\sigma_1^2 \geq \sigma_2^2 \ldots \geq \sigma_r^2 \geq \sigma_{r+1}^2 = \ldots = 0$.
On definit

$$Q \coloneqq \begin{pmatrix} u_1^* \\ \vdots \\ u_n^* \end{pmatrix}$$

Et soit

$$v_i \coloneqq \frac{Au_i}{\sigma_i}, \quad i = 1, \ldots, r$$

et on complete $v_1, \ldots, v_r$ *en une base orthogonale de* $\mathbb{C}^m$, *on va montrer que*

$$P \coloneqq (v_1, \ldots, v_r, v_{r+1}, \ldots, v_m) \in \mathbb{C}^{m \times m}$$

est unitaire.
Il est clair que $v_j^* v_j = 1 \forall j \geq r+1$, *sinon, pour* $1 \leq i, j \leq r$, *on a*

$$\begin{aligned} v_i^* v_j &= \frac{u_i^* A^*}{\sigma_i} \cdot \frac{A \cdot u_j}{\sigma_j} \\ &= \frac{u_i^* \sigma_j^2 u_j}{\sigma_i \sigma_j} \\ &= \begin{cases} 0 \ si \ i \neq j \\ 1 \ si \ i = j \end{cases} \end{aligned}$$

Il reste a verifier que

$$(P^* A Q^*)_{ij} = \begin{cases} 0 \ si \ i \geq r \ ou \ j > 0 \ ou \ i \neq j \\ \sigma_i \ autrement \end{cases}$$

Pour $i > r$ *et* $j \leq r$, *on a donc*

$$u_i^* A u_j = v_i^* \sigma_j v_j = 0$$

Et finalement, pour $i \leq j \leq r$, *on a*

$$= \frac{u_i^* A^*}{\sigma_i} A u_j$$

□

5.2 Pseudo-inverse d'une matrice

Definition 36 (Pseudo inerse)
Pour une matrice $A \in \mathbb{C}^{m \times n}$, *on note*

$$D^+ = \begin{pmatrix} \frac{1}{\sigma_1} & & \\ & \ddots & \\ & & \frac{1}{\sigma_r} \end{pmatrix} \in \mathbb{R}^{n \times m}$$

ou σ_i *sont les valeurs singulieres de* A.

Remarque
La factorisation en valeurs singulieres n'est pas unique.

On va montrer que le pseudo-inverse d'une matrice est unique.

Theorème 56
Soit $A \in \mathbb{C}^{m\times n}$, il existe au plus une seule matrice $X \in \mathbb{C}^{n\times m}$ qui satisfait les conditions de penrose

- $AXA = A$
- $(A \cdot X)^* = AX$
- $XAX = X$
- $(X \cdot A)^* = XA$

Preuve
Supposons que $X, Y \in \mathbb{C}^{n\times m}$ satisfait les conditions de penrose

$$\begin{aligned} X &= XAX \\ &= XAYAX \\ &= XAYAYAYAX \\ &= (XA)^*(YA)^*Y(AY)^*(AX)^* \\ &= A^*X^*A^*Y^*YY^*A^*X^*A^* \\ &= (AXA)^*Y^*YY^*(AXA)^* \\ &= A^*Y^*YY^*A^* \\ &= (YA)^*Y(AY)^* = YAYAY = YAY \end{aligned}$$ □

Theorème 57
Soit $A \in \mathbb{C}^{m\times n}$, alors A^+ verifie les regles de penrose.

Preuve
On verifie facilement pour D diagonale

—

$$AA^*A = PDQQ^*D^*P^*PDQ = PDQ = A$$ □

— *idem pour le reste.*

Lecture 17: Valeurs singulieres

Tue 27 Apr

$A \in \mathbb{C}^{m\times n}$, avec $A = PDQ^*$ avec D diagonale, P unitaire.
On a defini

$$A^+ = QD^+P^*$$

avec $D^+ = \begin{pmatrix} \frac{1}{\sigma_1} & & \\ & \ddots & \\ & & \frac{1}{\sigma_n} \end{pmatrix}$

5.3 Encore des systemes d'equation

On essaie a nouveau de resoudre

$$Ax = b, \quad A \in \mathbb{C}^{m\times n}, b \in \mathbb{C}^m$$

On veut trouver

$$\min_{x\in\mathbb{C}^n} \|Ax - b\|^2$$

On a, entre autre resolu $A^TAx = A^Tb$.
On va utiliser la pseudo-inverse de A pour trouver la solution.
On veut trouver $x \in \mathbb{C}^n$ la solution optimale tel que $\|x\|$ est optimale.

Theorème 58
Soit $A \in \mathbb{C}^{m\times n}, b \in \mathbb{C}^m$, alors $x = A^+b$ est une solution optimale de norme minimale parmi les solutions du systeme $Ax = b$.

Preuve
Soit $x \in \mathbb{C}^n$ et $Q \in \mathbb{C}^{n\times n}$ unitaire, alors

$$\|x\|^2 = x^*x = x^*Q^*Qx = \|Qx\|^2$$

On a donc

$$\begin{aligned} \min_{x\in\mathbb{C}^n} \|Ax - b\| &= \min_{x\in\mathbb{C}} \left\| PD \underbrace{Qx}_{:=y} - b \right\| \\ &= \min_{y\in\mathbb{C}^n} \|Dy - P^*b\| \\ &= \min_{y\in\mathbb{C}^n} \|Dy - c\| \end{aligned}$$ □

De plus y est une solution optimale $\iff y_{r+1} = \ldots = y_n = 0$
Et alors, $x = Q^*y = Q^*D^+P^*b$ est la solution optimale de norme minimale unique du probleme.

5.4 Le meilleur sous-espace approximatif

Etant donne $a_1, \ldots, a_m \in \mathbb{R}^n, 1 \le k \le n$.
On veut trouver un sous-espace $H \subseteq \mathbb{R}^n$, $\dim H \le k$ tel que

$$\sum_{i=1}^{m} d(H, \alpha_i)^2$$

est minimale.
On choisit une base orthonormale de $H : \{u_1, \ldots, u_k\}$, on peut facilement trouver la projection sur U, avec

$$proj(a_i) = \sum_{j=1}^{k} \langle \alpha_i, u_j \rangle \, u_j$$

Grace au theoreme de pythagore, on a

$$\|a_i\|^2 = \|proj(a_i)\|^2 + d(a_i, H)^2$$

Donc

$$\begin{aligned} \sum_{i=1}^{m} \|a_i\|^2 &= \sum_{i=1}^{m} \|proj(a_i)\|^2 + \sum_{i=1}^{m} d(a_i, H)^2 \\ &= \underbrace{\sum_{i=1}^{m} \sum_{j=1}^{k} (u_j^T a_i)^2}_{\text{A maximiser}} + \sum_{i=1}^{m} d(a_i, H)^2 \end{aligned}$$

On veut trouver un $H \subseteq \mathbb{R}^n$ tel que

$$\sum_{j=1}^{k} u_j^T A^T A u_j$$

avec $A = \begin{pmatrix} a_1^T \\ \vdots \\ a_m^T \end{pmatrix}$.
On veut maintenant trouver $H \subseteq \mathbb{R}^n, \dim H = k$ et avec n'importe quelle base orthogonale tel que

$$\sum_{j=1}^{k} u_j^T A^T A u_j$$

est maximale.

5.4.1 $k = 1$

On veut trouver

$$\max_{u \in S^{n-1}} u^T A^T A u$$

Avec le theoreme spectrale, on trouve la valeur propre maximale, et alors le sous-espace propre associe est solution. Par recurrence, on a

$$\begin{aligned} \sum_{j=1}^{k} w_j^T A^T A w_j &= \sum_{j=1}^{k-1} w_j^T A^T A w_j + w_k^T A^T A w_k \\ &\leq \sum_{j=1}^{k-1} u_j^T A^T A u_j + u_k^T A^T A u_k \end{aligned}$$

Lecture 18: Minimisation de la norme de Frobenius

Wed 28 Apr

Etant donne $A \in \mathbb{R}^{m\times n}, k \in \mathbb{N}$, on veuut trouver $B \in \mathbb{R}^{m\times n}$ tel que $rang(B) \leq k$ et

$$min_{C\in\mathbb{R}^{m\times n}, rangC\leq k} \|A - C\|_F$$

est atteint a B.

Definition 37 (Norme de Frobenius)
Soit $A \in \mathbb{R}^{m\times n}$,

$$\|A\|_F = \sqrt{\sum_{i,j} a_{i,j}^2}$$

Definition 38 (Trace)
$A \in K^{n\times n}$, la trace de A est definie par

$$Tr(A) = \sum_{i=1}^{n} a_{ii}$$

Lemme 59
On a

$$Tr(A \cdot B) = Tr(B \cdot A)$$

pour toute matrices dans $K^{n\times n}$

Preuve

$$\begin{aligned}(AB)_{ii} &= \sum_{k=1}^{n} a_{ik}b_{ki} \\ Tr(AB) &= \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} \\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik} = Tr(BA)\end{aligned}$$

□

Lemme 60
Soit $A \in \mathbb{R}^{m\times n}$, alors

$$\|A\|_F^2 = \sum_{i=1}^{r} \sigma_i^2$$

ou σ_i sont les valeurs singulieres.

Preuve

$$\begin{aligned} \|A\|_F^2 &= Tr(A^T A) \\ &= Tr(Q^T D^T P^T P D Q) \\ &= Tr(Q^T D^2 Q) \\ &= Tr(D^2) = \sum \sigma_i^2 \end{aligned}$$ □

On veut donc trouver $B \in \mathbb{R}^{m \times n}$ tel que

- $rang B \leq k$
- $\sum \|a_i - b_i\|^2$ est minimale

Pour $A \in \mathbb{R}^{m \times n}$, $A = PDQ$, avec $P = (v_1, \ldots, v_m)$ et $Q = \begin{pmatrix} u_1^T \\ \vdots \\ u_m^T \end{pmatrix}$.

Rappel : le span $\{u_1, \ldots, u_k\}$ minimise

$$\sum_{i=1}^{m} d(\alpha_i, H)^2$$

Definition 39
On definit

$$A_k = \sum_{i=1}^{k} v_i \sigma_i u_i^T$$

Clairement $rang(A_k) \leq k$.

Lemme 61
Les lignes de A_k sont les projections des lignes correspondantes de A dans le span $\{u_1, \ldots, u_k\}$.

Preuve
Soit a^T une ligne de A.
La projection

$$\tilde{A}^T = \sum_{i=1}^{k} (a^T u_i) u_i^T$$

Alors les projections de toutes les lignes de A sont

$$\sum_{i=1}^{k} A u_i u_i^T = \sum_{i=1}^{k} \sigma_i v_i u_i^T = A_k$$

Theorème 62
Soit $B \in \mathbb{R}^{m\times n}, rangB \leq k$ *alors*

$$\|A - A_k\|_F^2 \leq \|A - B\|_F^2$$

Preuve
Soit $A = \begin{pmatrix} a_1^T \\ \vdots \\ a_m^T \end{pmatrix}$, $B \begin{pmatrix} b_1^T \\ \vdots \\ b_m^T \end{pmatrix}$ *et* $A_k = \begin{pmatrix} \tilde{a}_1^T \\ \vdots\ \tilde{a}_m^T \end{pmatrix}$.
Soit $H = span\{b_1, \ldots, b_k'\}$ *sont une base de l'espace engendre par les lignes de* B, *alors*

$$\|A - B\|_F^2 = \sum_{i=1}^{m} \|a_i - b_i\|^2 \geq \sum_{i=1}^{m} d(a_i, H)^2$$

Soit $\tilde{H} = span\{u_1, \ldots, u_k\}$, *alors*

$$\sum_{i=1}^{m} d(a_i, H)^2 \geq \sum_{i=1}^{m} d(a_i, \tilde{H})^2 = \sum_{i=1}^{m} \|a_i - \tilde{a}_i\|_F^2$$

□

Lecture 19: Systemes differentiels lineaires

Tue 04 May

6 Systemes differentiels lineaires

Etant donne $a_{ij} \in \mathbb{R}, 1 \leq i \leq n, 1 \leq j \leq n$, on cherche une solution au systeme

$$\begin{cases} x_1'(t) = a_{11}x(t) + \ldots + a_{1n}x_n(t) \\ u\vdots \\ x_n'(t) = a_{n1}x(t) + \ldots + a_{nn}x_n(t) \end{cases}$$

On cherche $x_i : \mathbb{R} \to \mathbb{R}$ derivable qui resolvent le systeme d'equations lineaires.

Exemple

$$x'(t) = x(t)$$

Une solution est : $x(t) = e^t$.
Une autre est : $x(t) = 2e^t$.
Si on exige les conditions initiales $x(0) = 5$, *on aura la solution*

$$x(t) = 5e^t$$

Theorème 64
Etant donne les conditions initiales $x(0)$, il existe une solution unique qui respecte les conditions intiales.

On peut reecrire notre systeme comme

$$A \cdot x = x', A \in \mathbb{R}^{n \times n}$$

Supposons que $x(t) = ve^{\lambda t}$ est une solution du systeme($v \in \mathbb{R}^n$).
Alors,

$$x'(t) = A \cdot x(t) = \lambda v e^{\lambda t}$$

Donc v est un vecteur propre de A.

Lemme 65
Soit $\mathcal{X} = \{x : x$ solution du systeme differentiel $\}$, alors $\mathcal{X}$ est un espace vectoriel sur $\mathbb{R}$.

Theorème 66
Soit $\{v_1, \ldots, v_n\}$ une base de vecteurs propres de A associee aux valeurs propres $\lambda_1, \ldots, \lambda_n$.
Alors

$$x_i = e^{\lambda_i t} v_i, \quad i = 1, \ldots, n$$

est une base de $\mathcal{X}$.

Preuve
On a deja vu que x_i est une solution du systeme, car

$$A \cdot x_i = A v_i e^{\lambda_i t}$$

Soient $x(0) \in \mathbb{R}^n$ des conditions initiales, on veut trouver

$$\beta_1, \ldots, \beta_n \in \mathbb{R}^n \text{ tel que } \sum \beta_i x_i$$

est une solution qui respecte $x(0)$.
Soit $x(0) = \sum \beta_i x_i(0) = \sum \beta_i v_i$.
Cette combinaison lineaire existe car les v_i forment une base.
Supposons $\gamma_1, \ldots, \gamma_n \in \mathbb{R}$ tel que

$$\sum \gamma_i x_i(t) = 0$$

□

Considerons maintenant $A = P \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} P^{-1}$, ou $P \in \mathbb{C}^{n \times n}, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$.
Toute fonction $f : \mathbb{R} \to \mathbb{C}$ s'ecrit comme

$$f(t) = f_R(t) + i f_I(t)$$

avec $f_R, f_I : \mathbb{R} \to \mathbb{R}$.
f est derivable si f_R et f_I sont derivables.

Remarque
Si $x_1, \ldots, x_n : \mathbb{R} \to \mathbb{C}$ *sont derivables, alors* $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *est une solution du systeme si*

$$x' = A \cdot x$$

Lemme 68
Si $\lambda \in \mathbb{C}$ *est une valeur propre de* A *et si* $v \in \mathbb{C}^n \setminus \{0\}$ *un vecteur propre correspondant, alors*

$$x(t) = e^{\lambda t} v$$

est une solution complexe du systeme

Preuve

$$x' = \lambda e^{\lambda t} v = e^{\lambda t} A v = Ax$$ □

Lemme 69
Etant donne une solution complexe $x = x_R + ix_I$ *du systeme, alors* x_R *et* x_I *sont des solutions reelles du systeme.*

Preuve

$$x'_R + ix'_I = x' = Ax = Ax_R + iAx_I$$ □

Marche a suivre pour la resolution d'un systeme lineaire, avec valeurs propres complexes

— Soient $v_i = u_i + iw_i \in \mathbb{C}^n$ une base de vecteurs propres, alors on peut ecrire

$$v_{2j-1} = \overline{v}_{2j} \text{ et } \lambda_{2j-1} = \overline{\lambda}_{2j} \quad i \leq j \leq k \leq \frac{n}{2}$$

— $\{u_1, \ldots, u_k, w_1, \ldots, w_k, v_{2k+1}, \ldots, v_n\}$ une base de $\mathbb{R}^n u$
— Soit $v = u + iw$ une solution avec $\lambda = a + ib$

$$v = e^{\lambda t} v = e^{at}(\cos(bt) + i\sin(bt)) \cdot (u + iw)$$
$$= e^{at}\left((\cos(bt)u - \sin(bt)w) + (\sin(bt)u + \cos(bt)w)\right)$$

Lecture 21: forme normale de Jordan

Tue 11 May

Lemme 70
Pour $A, B \in \mathbb{C}^{n\times n}$, si $AB = BA$, alors

$$e^{A+B} = e^A e^B$$

On va montrer que pour chaque matrice $A \in \mathbb{C}^{n\times n}$ se laisse factoriser comme

$$A = P \cdot \left(\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} + N \right) \cdot P^{-1}$$

Ou P est inversible et $N \in \mathbb{C}^{n\times n}$ est nilpotente.
En effet, avec ce theoreme, on peut voir que

$$e^{tA} = Pe^{t(D+N)}P^{-1}$$

ou D est la matrice diagonale.
Un theoreme demontre en exercice donne alors

$$\begin{aligned} e^{tA} &= Pe^{t(D+N)}P^{-1} \\ &= Pe^{tD}e^{tN}P^{-1} \\ &= P \begin{pmatrix} e^{t\lambda_1} & & \\ & \ddots & \\ & & e^{t\lambda_n} \end{pmatrix} \left[\sum_{i=0}^{j} \frac{t^i}{i!} N^i \right] P^{-1} \end{aligned}$$

Definition 40 (Bloc de Jordan)
Un bloc de jorand est done par

$$\begin{pmatrix} \lambda_1 & 1 & & \\ & \ddots & 1 & \\ & & & \lambda_n \end{pmatrix}$$

Une matrice $A \in \mathbb{C}^{n\times n}$ est en forme normale de Jordan si

$$A = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{pmatrix}$$

ou les B_i sont des blocs de Jordan.

Lemme 71
Si $J \in K^{n\times n}$ est en forme noramle de Jordan et $J = D + N$, alors $DN = ND$.

Theorème 72
Soit $A \in K^{n\times n}$ et $m(x) \in K[x]$ un polynome avec coefficient dominant egal a 1.
De plus soit $m(A) = 0$.
Soit $\deg m$ minimal parmis tous les polynomes qui satisfont cette condition, alors $m(x)$ est unique et est appele polynome minimal de A.

Preuve
Soit $m'(x) \in K[x]$ aussi un tel polynome, cad $m'(A) = 0$, $\deg m' = \deg m$ et de coefficient dominant 1.
On va montrer que $m'|m$.
Par division euclidienne, on a

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

Or

$$m(A) = 0 = q(A)m'(A) + r(A) \Rightarrow r(A) = 0 \Rightarrow r = 0$$

Et donc $m = m'q \Rightarrow \deg q = 0$ □

Definition 41
Soit $A \in K^{n\times n}$ une matrice.
Soit $W \subset K^n$, W est invariant sur A, si $\forall w \in W, A \cdot w \in W$

Lemme 73
Soit $f(x) \in K[x]$ et $A \in K^{n\times n}$, soit $v \in \ker f(A)$, alors $Av \in \ker f(A)$.
cad que $\ker f(A)$ est invariant sur A.

Preuve
A montrer : pour $v \in K^n$, si $f(A)v = 0$, alors

$$f(A)Av = 0$$

Mais $f(A)Av = Af(A)v = 0$ □

Lecture 22: calcul de la forme normale d eJordan

Wed 12 May

On souhaite demontrer que toute matrice $A \in \mathbb{C}^{n\times n}$ se laisse ecrire comme

$$A = P^{-1}(D + N)P$$

avec N nilpotente , P inversible, D diagonale et $DN = ND$.

Lemme 74
Soient $p(x), q(x) \in K[x]$ tel que $gcd(p,q) = 1$ et soit $A \in K^{n\times n}$, alors

$$K^n \supset \ker(pq(A)) = \ker p(A) \oplus \ker q(A)$$

Preuve
Par hypothese, il existe $g, h \in K[x]$ tel que

$$gp + hq = 1$$

Donc

$$\mathrm{Id} = gp(A) + hq(A) \tag{1}$$

Soit $v \in \ker(pq(A))$, donc on a

$$v = \underbrace{gp(A)v}_{\in \ker(q(A))} + hq(A)v$$

Soit $v \in \ker q(A) \cap \ker p(A)$, alors

$$\mathrm{Id}\, v = gp(A)v + hq(A)v = 0 \Rightarrow v = 0$$

Donc la somme est directe. □

Corollaire 75
Soient $p_1, \ldots, p_k \in K[x]$ tel que $gcd(p_1, \ldots, p_k) = 1$.
Donc $\ker\left(\prod_{i=1}^k p_i(A)\right) = \ker p_1(A) \oplus \ldots \oplus \ker(p_k(A))$.

Supposons que $K^n = \ker\left(\prod_{i=1}^q p_i(A)\right)$.
Supposons qu'on aie une base de $\ker p_i(A) = \left\{v_j^{(i)}, 0 < j \leq n_1\right\}$

$$K^{n\times n} \ni V = \left[v_1^{(1)}, \ldots, v_{n_k}^k\right]$$

Theorème 76
Soit $A \in \mathbb{C}^{n\times n}$, il existe $P \in \mathbb{C}^{n\times n}$ inversible tel que

$$A = P^{-1}(D + N)P$$

ou N est nilpotente.

Preuve
Soit $m(x) \in \mathbb{C}[x]$ le polynome minimal de A, alors

$$m(x) = \prod_{i=1}^k (x - \lambda_i)^{m_i}$$

On sait que

$$\mathbb{C}^n = \ker(m(A)) = \bigoplus \ker(A - \lambda_i)^{m_i}$$

On pose P la matrice qui contient les bases de tous les espaces.

$$P^{-1}AP - \lambda_1 \operatorname{Id} = P^{-1}(A - \lambda_1 \operatorname{Id})P$$

Eleve a la puissance m_1, on trouve

$$\begin{aligned}(P^{-1}AP - \lambda_1 \operatorname{Id})^{m_1} &= P^{-1}(A - \lambda_1 \operatorname{Id})^{m_1} P \\ &= P^{-1}[\underbrace{0}_{n_1} | X]\end{aligned}$$

Alors $(B_1 - \lambda_1 \operatorname{Id}_{n_1})^{m_1} = 0$, et de maniere plus generale

$$(B_i - \lambda_i \underset{n_i}{\operatorname{Id}})^{m_i} = 0$$

On en deduit que

$$P^{-1}AP = N + D$$

Et N est nilpotent, car

$$N^{\max\{m_1,\dots,m_k\}} = 0$$

□

Theorème 77
Soit $N \in K^{n\times n}$ nilpotente, alors $\exists P \in K^{n\times n}$ inversible tel que

$$P^{-1}NP$$

est en forme normale de Jordan avec des 0 sur la diagonale.

Lecture 23: forme normale de Jordan

Tue 18 May

On cherche une base tel que les N_i de la decomposition en forme de Jordan aient des 1 dans la diagonale superieure. Ainsi, on aura bel et bien que $DN = ND$.

Theorème 78
Soit $N \in K^{n\times n}$ une matrice nilpotente.
Alors, il existe $P \in K^{n\times n}$ tel que

$$P^{-1}NP$$

est en forme normale de Jordan.

Alors, en utilisant ce resultat, on pose

$$\begin{pmatrix} P_1^{-1} & & \\ & \ddots & \\ & & P_k^{-1} \end{pmatrix} P^{-1}AP \begin{pmatrix} p_1 & & \\ & \ddots & \\ & & P_k \end{pmatrix}$$

Dans les blocs, on aura donc des elements de la forme

$$P_i^{-1}(\lambda_i \operatorname{Id} + N_i)P_i$$

Theorème 79

Soit $N \in K^{n\times n}$ nilpotente, il existe une base B de K^n de la forme

$$x_1, Nx_1, \ldots, N^{m_1-1}x_1, \ldots N^{m_n-1}x_n$$

tel que $N^{m_i}x_i = 0$. En inversant l'ordre de la base, on obtient la matrice de passage desiree.

Preuve
Pour $x \in K^{n\times n} \setminus \{0\}$, on appelle la duree de vie de x :

$$\min_{N^j x \neq 0} = m_x$$

On appelle l'orbite de x :

$$x, Nx, \ldots, N^{m_k-1}x$$

Posons E pour la concatenation des orbites.
Invariante :
On va maintenir $x_1, \ldots, x_k \in K^n$ tel que les orbites concatenees des x_i engendrent K^n.
Posons $x_i = e_i, k = n$, on a clairement que la concatenation des orbites engendre K^n.

- *Si E est lineairement dependante on va remplacer un x_i par y d'une telle maniere que l'invariante est satisfaite. Ou bien effacer un x_i tel que l'invariante est satisfaite.*

On suppose E lineairement dependant, alors

$$\beta_0^1 x_1 + \ldots + \beta^1_{m_{x_1}-1}N^{m_{x_1}-1} + \ldots + \beta_{m_{x_k}-1}N^{m_{x_k}}x_k = 0 \quad (*)$$

est une cl non triviale.

- *Cas 1 : $\exists i$ tel que $m_{x_i} = 1$, $\beta_0^1 \neq 0$.*
  Alors l'orbite de x_i est dans le span des orbites de $x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_k$
  Alors on efface x_i
- *Cas 2 : Maintenant, on applique N a $(*)$ tel que pas tous les $\beta_i^j N^k N^i x_j = 0$*

Cette demarche nous donne un sous-ensemble $J \subset [k]$ et $\gamma_j \neq 0, j \in J$ tel que

$$\sum_{j\in J} \gamma_j N^{m_{x_j}-1}x_j = 0$$

Soit $m = \min_{j \in J} m_{x_j}$ *et* $i \in J$ *un index ou le min est atteint. Alors on a*

$$0 = N^{m_{x_i}-1} \left(\sum_{j \in J, j \neq i} \gamma_j N^{m_{x_j}-1-m_{x_i}+1} x_j + \gamma_i x_i \right) \qquad \square$$

Lecture 24: algebre lineaire sur les entiers

Wed 19 May

7 Algebre lineaire sur les entiers

But :
Etant donne $A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m$, on veut trouver $x \in \mathbb{Z}^n$ tel que

$$Ax = b$$

Si $m = n$, $\det A \neq 0$, alors on a une solution rationelle de la forme

$$x = A^{-1}b$$

Dans ce cas, le systeme $Ax = b$ est resoluble si et seulement si $A^{-1}b \in \mathbb{Z}^m$.
Mais que fait-on si le systeme est sous-determine ?
Un probleme plus specifique, discute pour la premiere fois par Gauss est

$$a, b, c \in \mathbb{Z} \setminus \{0\}$$

$$ax + by = c, x, y \in \mathbb{Z}.$$

Le systeme est soluble si et seulement si $\gcd(a, b)|c$

Preuve
$\Rightarrow$ *Supposons* $d|a, d|b$.
Soit $x, y \in \mathbb{Z}$ *une solution du systeme*

$$xa + yb = c$$
$$d(xa' + yb') = c \Rightarrow d|c \Rightarrow \gcd(a, b)|c$$

$\Leftarrow \exists x', y' \in \mathbb{Z}$ *tel que* $\gcd(a, b) = d = x'a + y'b$ $\square$

Un algorithme pour trouver la solution est l'algorithme d'Euclide.

7.1 Forme normale d'Hermite

On veut resoudre des systemes de la forme $Ax = b, x \in \mathbb{Z}^n$.
On veut trouver $Q \in \mathbb{Q}^{n \times n}$ inversible tel que

$$Aq = T$$

Ou T est une matrice triangulaire inferieure triangulaire.

Definition 42 (Matrice unimodulaire)
Une matrice $Q \in \mathbb{Z}^{n\times n}$ *est unimodulaire si* $\det Q = \pm 1$.

Lemme 80
Soit $Q \in \mathbb{Z}^{n\times n}, \det Q \neq 0$, *alors* $Q^{-1} \in \mathbb{Z}^{n\times n} \iff Q$ *est unimodulaire.*

Preuve
$\Leftarrow$
On a

$$Q^{-1} = \frac{1}{\det Q}\tilde{Q}^T$$

Or la matrice des cofacteurs possede comme composantes des determinants de matrices $(n-1)\times(n-1)$ *sous-matrices de* Q.
Mais $\det A \in \mathbb{Z}$ *pour* $A \in \mathbb{Z}, \det A = \sum_{\sigma\in S_n} sign(\sigma)\prod_{i=1}^{n} a_{i\sigma(i)}$.
Donc l'inverse de la matrice est une matrice integrale.
$\Rightarrow$

$$\mathrm{Id} = \det \mathrm{Id} = \det QQ^{-1} = \det Q \det Q^{-1}$$

Il en suit le theoreme. □

Donc, pour revenir au probleme $Ax = b, x \in \mathbb{Z}^n$, on a

$$AUU^{-1}x = b$$

Donc $x \in \mathbb{Z}^n$ est solution du systeme si et seulement si

$$U^{-1}x \in \mathbb{Z}$$

est solution de $AU = b$. Ajouter un multiple entier d'une colonne a une autre colonne.

Lecture 25: systemes d equations diophantiennes

Tue 25 May

Soit $Ax = b, x \in \mathbb{Z}^n, A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$.
On va supposer que $rang A = m$.

Lemme 81
Soit $U \in \mathbb{Z}^{n\times n}$ *inversible (sur* $\mathbb{Q}$ *) :*

$$U^{-1} \in \mathbb{Z}^{n\times n} \iff \det U = \pm 1$$

U *est unimodulaire.*

On veut donc trouver un $U \in \mathbb{Z}^{n\times n}$ unimodulaire tel que

$$AU = [H|0], \text{ ou } H \in \mathbb{Z}^{m\times m} \text{ inversible}$$

On a donc

$$\begin{aligned} & Ax = b, x \in \mathbb{Z}^n \text{ solution} \\ \iff & AUy = b, y \in \mathbb{Z}^n \text{ solution} \end{aligned}$$

Ou $y = U^{-1}x$.
On dit que AU est en forme normale d'Hermite si $h_{ij} < h_{ii}$ pour tout $i = 1, \ldots, m, j = 1, \ldots, i-1$.
En consequence,

$$AU = [H|0] \text{ en FNH}$$

tel que

$$Ax = b, x \in \mathbb{Z}^n \text{ solution} \iff Hy = b, y \in \mathbb{Z}^m$$

Lemme 82
Soit $(a_1, \ldots, a_n) \in \mathbb{Z}^{1\times n} \setminus \{0\}$ *, alors* $\exists U \in \mathbb{Z}^{n\times n}$ *tel que*

$$(a_1, \ldots, a_n) \cdot U = (\gcd(a_1, \ldots, a_n), 0, \ldots, 0)$$

Preuve
Recurrence sur le nombre de composantes $\neq 0$ $n = 1$
On multiplie eventuellement avec -1 *pour obtenir le gcd et on echange les lignes avec les collonnes.* $n > 1$
Soient $a_i, a_j \neq 0$, $j \neq i$, *on multiplie*

$$(\ldots, a_i, \ldots, a_j, \ldots) \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

avec x *dans la* i, i *-eme composante,* y *dans la* i, j *-eme composante,* $-\frac{a_i}{d}$ *dans la* j, j *composante et* $\frac{a_j}{d}$ *dans la* j, i *-eme composante.*
Et car

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c)$$ □

On conclut par recurrence.

Theorème 83
Soit $A \in \mathbb{Z}^{m\times n}, rangA = m$ *, alors* $\exists U \in \mathbb{Z}^{m\times n}$ *tel que* AU *est en forme normale de Hermite.*

Preuve
On montre a nouveau par recurrence sur m .
$m = 1$
Vrai par le lemme ci-dessus.

$m > 1$

Par le lemme, il existe U tel que

$$AU = \begin{pmatrix} \gcd(a_{11}, \ldots) & 0 & & \\ a_{21} & A' & a_{21} & a_{21} \end{pmatrix}$$

Pour $m > 1$, par recurrence, $\exists U' \in \mathbb{Z}^{k-1 \times n-1}$ unimodulaire tel que

$$A'U' = [H'|0]$$ □

Lemme 84
Soit $A \in \mathbb{Z}^{m \times n}, rangA = m$.
La FNH de A est unique.

Preuve
Soient $U_1, U_2 \in \mathbb{Z}^{n \times n}$ unimodulaire et $H_1 \neq H_2 \in \mathbb{Z}^{m \times m}$ en FNH tel que

$$AU_1 = [H_1|0], AU_2 = [H_2|0]$$

Alors

$$A\mathbb{Z}^n = \{Ax : x \in \mathbb{Z}^n\} = H_1\mathbb{Z}^m = H_2\mathbb{Z}^m$$

Soit $i \in \{1, \ldots, m\}$ minimal tel qu'il existe $j \in \{1, \ldots, i\}$ tel que $h_{ij} \neq h'_{ij}$, sans perte de généralité $h_{ij} > h'_{ij}$.
Soient $h \in \mathbb{Z}^m, h' \in \mathbb{Z}^m$ les j-emes colonnes de H_1 et H_2 respectivement.
Alors on a

$$h - h' = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ h_{ij} - h'_{ij} \\ \vdots \end{pmatrix}$$

$\exists y_1, y_2 \in \mathbb{Z}^m : H_1 y_1 = H_2 y_2 = h - h'$.
Alors

$$h_{ij} - h'_{ij} = z_1 h_{ii} = z_2 h'_{ii}, z_1, z_2 \in \mathbb{Z} \setminus \{0\}$$

Donc

$$\Rightarrow h_{ij} - h'_{ij} \geq h_{ii}$$
$$\Rightarrow h_{ij} - h'_{ij} \geq h'_i i$$

Si $i = j$, alors $h'_{ij} \neq 0$, alors

$$h_{ij} - h'_{ij} < h_{ij} \lightning$$

Si $i > j$

$$h_{ij} - h'_{ij} < h_{ii} \lightning$$ □

8 La forme normale de Smith

Theorème 85
Soit $A \in \mathbb{Z}^{m\times n}$.
Il existe $U \in \mathbb{Z}^{m\times m}, V \in \mathbb{Z}^{n\times n}$ *unimodulaires tel que*

$$UAV = D$$

est diagonale, ou $d_i | d_{i+1}$ *et* $d_i \in \mathbb{N} \forall i$

Preuve
On veut transformer A *en une matrice de la forme*

$$\begin{pmatrix} d & 0 \\ 0 & A' \end{pmatrix}$$

tel que d *divise chaque composante de* A'.
Si $A' = 0$ *et on a fini.*
Autrement $U' \in \mathbb{Z}^{m-1\times m-1}$ *et* $v' \in \mathbb{Z}^{n-1\times n-1}$ *unimodulaire tel que*

$$U'A'V' = D'$$

On va identifier l'element non nul de la premiere ligne ou colonne de $A \neq_0$ *de valeur absolue minimale.*
Si l'element pivot ne divise pas tous les autres elements de A*, on transforme* A *tel que le nouvel element pivot est plus petit.*
Si $a_{11} \not| a_{1j} \Rightarrow a_{1j} = qa_{11} + r$ *, avec* $0 < r < a_{11}$.
On soustrait q *fois la colonne* 1 *de* A *de la colonne* j.
ainsi, $0 < a_{1j} < a_{11}$
Ensuite en echange la colonne 1 *et* j *et le nouvel element pivot est plus petit.*
Sinon, $a_{11} | a_{i_1}, i > 1$
Si $a_{11} | a_{1i} \forall i = 2, \ldots, a_{11} | a_{1j} \forall j = 2, \ldots i$
Ainsi, on peut eliminer tous les elements sur la premiere ligne et sur la premiere colonne.
Supposons donc que $a_{11} \not| a_{ij}$ *, alors on ajoute la* i *-eme ligne a la premiere ligne et on effectue la division euclidienne.* □