

162 - Systèmes d'équations linéaires; opérations élémentaires, aspects algorithmiques, conséquences théoriques

I - THÉORIE GÉNÉRALE DES SYSTÈMES LINÉAIRES. [GOU] [GRI] [RDO]

Cadre: K est un corps - On cherche à résoudre $AX = b$ où $A \in \mathcal{M}_{m,n}(K)$ et $b \in \mathcal{M}_{m,1}(K)$.

Déf 1: Le système est compatible lorsqu'il admet au moins une solution $X \in \mathcal{M}_{n,1}(K)$. Le rang du système est le rang de A .

1 - Systèmes de Cramer.

Déf 2. Lorsque $A \in GL_n(K)$, on parle de système de Cramer.

Rem 3. Un système de Cramer admet une unique solution $X = A^{-1}b$.

Théorème 4. En notant $A = (a_{ij})_{1 \leq i, j \leq n}$, l'unique solution du système de Cramer $AX = b$ est donnée par $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ où pour $i \in \{1, \dots, n\}$,

$$x_i = \frac{\begin{vmatrix} a_{11} & \dots & a_{1i} & \dots & a_{1n} & b_1 - a_{1i}x_i \\ \vdots & & \vdots & & \vdots & \vdots \\ a_{i1} & \dots & a_{ii} & \dots & a_{in} & b_i - a_{ii}x_i \\ \vdots & & \vdots & & \vdots & \vdots \\ a_{n1} & \dots & a_{ni} & \dots & a_{nn} & b_n - a_{ni}x_i \end{vmatrix}}{\det A}$$

Rem 5. Le calcul de la solution demande de l'ordre de $(n+1)!$ opérations.

Exemple 6: Dans \mathbb{R} , si $A = \begin{pmatrix} 2 & -5 & 2 \\ 1 & 2 & -4 \\ 3 & -4 & -6 \end{pmatrix}$ et $b = \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix}$, on a:

$$x_1 = -\frac{1}{46} \begin{vmatrix} 7 & -5 & 2 \\ 3 & 2 & -4 \\ 5 & -4 & -6 \end{vmatrix} = 5; \quad y = -\frac{1}{46} \begin{vmatrix} 2 & 7 & 2 \\ 1 & 3 & -4 \\ 3 & 5 & -6 \end{vmatrix} = 1; \quad z = -\frac{1}{46} \begin{vmatrix} 2 & -5 & 7 \\ 1 & 2 & 3 \\ 3 & -4 & 5 \end{vmatrix} = 1.$$

2 - Cas général - Théorème de Rouché-Fontené

Cadre: $A \in \mathcal{M}_{m,n}(K)$, $r \in \mathbb{N}$, $\{r, \min(n,m)\}$ le rang du système.

Quitte à permuter et renumérotter les équations, on peut supposer que:

$$\delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0.$$

Déf 7: On appelle déterminants caractéristiques les déterminants:

$$\Delta_s = \begin{vmatrix} a_{11} & \dots & a_{1r} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{r1} & \dots & a_{rr} & b_r \\ a_{s,1} & \dots & a_{s,r} & b_s \end{vmatrix} \quad \text{pour } s \in \{r+1, \dots, n\}$$

Théorème 8 (Rouché-Fontené). Le système est compatible si et seulement si $\Delta_s = 0$ pour tout $s \in \{r+1, \dots, n\}$. Dans ce cas, le système est équivalent à

$$\begin{cases} a_{11}x_1 + \dots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \dots - a_{1,n}x_n \\ \vdots \\ a_{r,1}x_1 + \dots + a_{r,r}x_r = b_r - a_{r,r+1}x_{r+1} - \dots - a_{r,n}x_n \end{cases}$$

Les solutions forment un espace affine de dimension $n-r$ et dépendent des paramètres x_{r+1}, \dots, x_n .

Exemple 9. Dans \mathbb{R} , soit $A = \begin{pmatrix} 1 & 2 & -1 & 1 \\ 1 & 0 & -1 & -1 \\ -1 & 1 & 1 & 2 \end{pmatrix}$ et soit $b = \begin{pmatrix} 1 \\ 1 \\ m \end{pmatrix}$, $m \in \mathbb{R}$.

$\text{rang}(A) = 2$, le seul déterminant caractéristique est:

$$\Delta = \begin{vmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ -1 & 1 & m \end{vmatrix} = -2(m+1).$$

Le système admet des solutions ssi $m = -1$ et dans ce cas il est équivalent à $\begin{cases} x_1 = 1 + x_3 + x_4 \\ x_2 = -x_4 \end{cases}$.

3 - Le cas des systèmes homogènes. [JL]

Cadre: $A \in \mathcal{M}_{m,n}(K)$ et $b = 0$.

Proposition 10. Si le système est de rang r , alors les solutions forment un espace vectoriel de dimension $n-r$.

lemme 11 (Dedekind). (Un système) une famille de r automorphismes de corps est toujours de rang r . DÉVELOPPEMENT

lemme 12 (Artin). Soient \mathbb{K} un corps et H un sous-groupe fini de $\text{Aut}(\mathbb{K})$. Alors \mathbb{K}/\mathbb{K}^H est une extension finie de degré $[\mathbb{K}:\mathbb{K}^H] = |H|$.

Corollaire 13. Sous les hypothèses du lemme d'Artin, $H = \text{Aut}(\mathbb{K}/\mathbb{K}^H)$.

II - SUR LES OPÉRATIONS ÉLÉMENTAIRES

1 - Définitions [RDO], [H2&2]

Déf 14: Soit $p \in \mathbb{N}^*$. On définit les matrices $p \times p$ dites élémentaires:

dilatation : $i \in \{1, \dots, p\}, \alpha \in \mathbb{K}^*$, $D_i(\alpha) := \begin{pmatrix} \alpha & & & \\ & \ddots & & \\ & & \alpha & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$

transvection : $i, j \in \{1, \dots, p\}, \lambda \in \mathbb{K}$, $T_{ij}(\lambda) := \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$

permutation : $i, j \in \{1, \dots, p\}$, $P_{ij} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$

Proposition 15 : Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$. On note L_i la i -ème ligne de \mathbb{K} . Si $p = m$, la multiplication à gauche par une matrice élémentaire donne :

opération	$D_i(\alpha)A$	$T_{ij}(\lambda)A$	$P_{ij}A$	idem sur les colonnes de A en multipliant à droite.
resultat	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftrightarrow L_j$	

Lemme 16. Les matrices élémentaires sont inversibles avec :

$$D_i(\alpha)^{-1} = D_i\left(\frac{1}{\alpha}\right) ; T_{ij}(\lambda)^{-1} = T_{ij}(-\lambda) ; P_{ij}^{-1} = P_{ij}$$

Théorème 17. Les matrices de transvection de taille n engendrent $SL_n(\mathbb{K})$.
• Les matrices de transvection et de dilatation de taille n engendrent $GL_n(\mathbb{K})$.

Application 18 : $GL_n(\mathbb{C}), SL_n(\mathbb{C}), SL_n(\mathbb{R})$ sont connexes par arcs.

$GL_n(\mathbb{R})$ a deux composantes connexes par arcs :
 $GL_n^+(\mathbb{R}) := \{M \in GL_n(\mathbb{R}), \det M > 0\}$ et $GL_n^-(\mathbb{R}) := GL_n(\mathbb{R}) \setminus GL_n^+(\mathbb{R})$.

2. L'algorithme du pivot de Gauss [R00], [ALL]

Lemme 19. Toute matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ à première colonne non nulle peut être transformée par multiplication à gauche par des transvection en une matrice de la forme $\begin{pmatrix} \beta & * & \dots & * \\ \vdots & \tilde{A} & & \\ 0 & & & \end{pmatrix}$, $\tilde{A} \in \mathcal{M}_{m-1, n-1}(\mathbb{K})$.

Corollaire 20. Soit $A \in \mathcal{M}_n(\mathbb{K})$. Il existe $M \in GL_n(\mathbb{K})$ qui est un produit de matrices de transvection triangulaires supérieures et de matrices de permutation telle que $T := MA$ soit triangulaire supérieure.

Algorithme 21. Pour p de 1 à n faire :

- si $a_{pp} \neq 0$, annuler les a_{jp} , $j > p$ en multipliant par $T_{jp}\left(-\frac{a_{jp}}{a_{pp}}\right)$
- si $a_{pp} = 0$, permuter $L_p \leftrightarrow L_j$, $j > p$ telle que $a_{jp} \neq 0$. Si une telle ligne n'existe pas, passer à l'étape suivante.

Application 22 : Avec les notations précédentes, le système $AX = b$ est équivalent à $TX = Mb$.

Application 23 (Bruhat). \mathcal{T}_s désigne le groupe des matrices triangulaires supérieures inversibles sur \mathbb{K}^n . On a : $GL_n(\mathbb{K}) = \coprod_{s \in \mathcal{S}_n} \mathcal{T}_s P_s \mathcal{T}_s$. [F&N]

Rem 24 : L'algorithme du pivot de Gauss nécessite $\mathcal{O}(n^3)$ opérations.

3. En termes d'actions de groupe [H2&2]

Cadre : Étudier les orbites de l'action de $GL_m(\mathbb{K})$ sur $\mathcal{M}_{m,n}(\mathbb{K})$ par multiplication à gauche.

Def. 25. Dans $\mathcal{M}_{m,n}(\mathbb{K})$, on appelle pivot d'une ligne le coefficient non nul (s'il existe) situé dans la colonne la plus à gauche. Une matrice est dite échelonnée réduite lorsqu'elle vérifie les conditions :

- si une ligne est nulle, toutes les lignes suivantes sont nulles.
- le pivot d'une ligne est strictement plus à droite que ceux des lignes précédentes.
- tous les pivots sont égaux à 1 et sont les seuls coefficients non nuls de leur colonne.

Exemple 26 : $\begin{pmatrix} 0 & 1 & 0 & * & 0 & * & * \\ 0 & 0 & 1 & * & 0 & * & * \\ 0 & 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ est échelonnée réduite.

NOTATION : On note $\mathcal{E}_{m,n}$ l'ensemble des matrices échelonnées réduites de $\mathcal{M}_{m,n}(\mathbb{K})$.

Théorème 27. Soient $A, A' \in \mathcal{M}_{m,n}(\mathbb{K})$. A et A' sont dans la même orbite pour l'action par multiplication à gauche ssi $\text{Ker } A = \text{Ker } A'$.
On a : $\mathcal{M}_{m,n}(\mathbb{K}) = \coprod_{E \in \mathcal{E}_{m,n}} \text{Orb}(E)$.

Rem. 28 : On peut conduire la même étude pour l'action par multiplication à droite.

4- Sur un anneau euclidien. [BMP]

Lemme 29. Soit A un anneau euclidien et $M \in \mathcal{M}_n(A)$. Il existe δ un pgcd des éléments de M et $M' \in \mathcal{M}_{n-1}(A)$ tels que M soit équivalente à la matrice $\begin{pmatrix} \delta & 0 & \dots & 0 \\ \vdots & \delta M' & & \end{pmatrix}$.

Théorème 30. Soit A un anneau euclidien. Soient L un A -module de rang n et $R \subset L$ un sous A -module. Il existe une base (e_1, \dots, e_n) de L (base adaptée) et $(d_1, \dots, d_k) \in A^k$ tels que $d_1 | d_2 | \dots | d_k$ et $(d_1 e_1, \dots, d_k e_k)$ est une base de R .

Application 31. Classification des groupes abéliens finis.

III - RÉSOLUTION EFFECTIVE DES SYSTÈMES LINÉAIRES

Proposition 32. La résolution d'un système triangulaire supérieur demande $\mathcal{O}(n^2)$ opérations.

Définition 33. Le conditionnement de $A \in \mathcal{M}_n(\mathbb{C})$ relativement à la norme subordonnée $\|\cdot\|$ est $\text{cond}(A) = \|A\| \|A^{-1}\| \geq 1$.

Proposition 34. Si $Ax = b$ et $A(x + \delta x) = b + \delta b$, alors $\frac{\|\delta x\|}{\|x\|} \leq \text{cond}(A) \frac{\|\delta b\|}{\|b\|}$.

Si $(A + \delta A)(x + \delta x) = b$, alors $\frac{\|\delta x\|}{\|x + \delta x\|} \leq \text{cond}(A) \frac{\|\delta A\|}{\|A\|}$.

Ces inégalités sont optimales.

1- Méthodes directes [ALL], [CIA], [QSS]

Cadre: Solution "exacte" en un nombre fini d'étapes.

Théorème 35 (LU) Soit $A \in GL_n(\mathbb{C})$ telle que tous ses mineurs principaux soient non nuls. Il existe un unique couple (L, U) avec U triangulaire supérieure et L triangulaire inférieure ayant une diagonale de 1 tel que $A = LU$. Le calcul est explicite par l'algorithme de Gauss "sans permuter".

Application 36: $Ax = b \Leftrightarrow \begin{cases} Ux = y \\ Ly = b \end{cases}$. Il y a $\mathcal{O}(n^3)$ opérations.

Déf. 37: Une matrice A est dite bande $p \in \mathbb{N}$ lorsque $a_{ij} = 0$ pour $|i-j| > p$.

Proposition 38: La factorisation LU conserve la structure bande des matrices.

Application 39: Factorisation LU d'une matrice tridiagonale en $\mathcal{O}(n)$ opérations.

Théorème 40 (QR) Soit $A \in \mathcal{M}_{m,n}(\mathbb{C})$. Il existe $Q \in \mathcal{M}_m(\mathbb{C})$ unitaire et $R \in \mathcal{M}_{m,n}(\mathbb{C})$ triangulaire supérieure telle que $A = QR$.

Application 41. Si $A \in GL_n(\mathbb{C})$, $Ax = b \Leftrightarrow Rx = Q^* b$.

Rem 42: On peut obtenir la factorisation QR par l'algorithme de Gram-Schmidt.

2- Méthodes itératives, épisode 1 [CIA] DÉVELOPPEMENT

Cadre: Construire une suite $(x_k)_k$ qui converge vers la solution de $Ax = b$.

Théorème 43. Si $A = M - N$ avec $M \in GL_n(\mathbb{C})$ et $N \in \mathcal{M}_n(\mathbb{C})$, la suite :

$$\begin{cases} x_0 \in \mathbb{C}^n \\ x_{k+1} = M^{-1}(Nx_k + b) \end{cases} \text{ converge vers } x \text{ tq } Ax = b \text{ ssi } \rho(M^{-1}N) < 1.$$

Exemples 44. En particulier, sont utilisées :

• Méthode de Jacobi: $M = \text{diag}(a_{11}, \dots, a_{nn}) = D$ et $N = D - A$.

• Méthode de Gauss-Jacobi: $M = D - E$ où $E = -A_{\text{inf}}$ \rightarrow partie triangulaire inf sup et inf strictes.

• Méthode SOR: $M = \frac{D}{\omega} - E$, $N = \frac{1-\omega}{\omega} D + F$, $\omega \in \mathbb{C}$.

But: trouver ω optimal pour converger plus rapidement.

3- Méthodes itératives, épisode 2: méthodes de gradient. [LAX], [QSS]

Cadre: $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

Théorème 45: La solution de $Ax = b$ minimise $E(y) = \frac{1}{2} \langle y, Ay \rangle - \langle y, b \rangle$.

Définition 46. On appelle méthode de gradient une méthode itérative de la forme $x_0 \in \mathbb{R}^n$, $x_{k+1} = x_k + \alpha_k d_k$ où $\alpha_k = \frac{\langle d_k, r_k \rangle}{\|d_k\|_A^2}$ où $r_k = b - Ax_k$ et $\| \cdot \|_A = \langle \cdot, A \cdot \rangle$.

Théorème 47: $\|x_{k+1} - x_k\|_A^2 = (1 - \beta_k) \|x_k - x\|_A^2$ où $\beta_k = \frac{\langle d_k, r_k \rangle}{\|d_k\|_A^2 \|r_k\|_A^2} \in [0, 1]$.

Exemples 48. En particulier, sont utilisées :

• Gradient pas optimal: $d_k = r_k$ alors $\|x_k - x\| \leq \text{cond}(A) \left(\frac{\text{cond}(A) - 1}{\text{cond}(A) + 1} \right)^k \|x_0 - x\|$.

• Gradient conjugué: $d_{k+1} = r_{k+1} - \beta_k d_k$ où $\beta_k = \frac{\langle r_{k+1}, A d_k \rangle}{\|d_k\|_A^2}$.

Théorème 49: La méthode de gradient conjugué converge en au plus n itérations vers x .

ANNEXE : ILLUSTRATIONS POUR LES MÉTHODES DE GRADIENT

On représente les courbes de niveau de $E(y) = \frac{1}{2} \langle y, Ay \rangle - \langle y, b \rangle$.

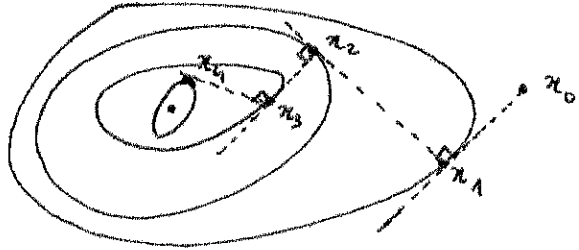


Figure 1 : Gradient à pas optimal



Figure 2 : Gradient à pas optimal : une mauvaise situation.

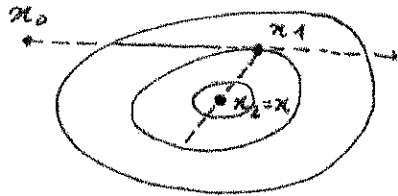


Figure 3 : Gradient conjugué en dimension 2.

BIBLIOGRAPHIE

- [ALL] Grégoire ALLAIRE, Analyse numérique et optimisation, 2^e édition
- [BMP] V. BECK, J. MALICK, G. PEYRÉ, Objectif Agrégation
- [H2G2] P. CALDERO, J. GERMONI, Histoires Hédonistes de Groupes et de Géométries, T.1
- [CIA] P.G. CIARLET, Introduction à l'Analyse numérique matricielle
- [GOU] X. GOURDON, Les maths en tête : Algèbre
- [GRI] J. GRIFONE, Algèbre Linéaire, 4^e éd.
- [JL] A. JEANNERET, D. LINES, Invitation à l'algèbre
- [LAX] P.D. LAX, Linear Algebra and its Applications, 2nd ed.
- [QSS] A. QUATERONI, R. SACCO, F. SALERI, Numerical Mathematics
- [RDO] E. RAMIS, C. DESCHAMPS, J. ODOUX, Cours de Maths. Spéciales T.1.

Antoine DIEZ
Gabriel LEPETIT

Théorème d'Artin

Gabriel Lepeitit, Antoine Diez

Théorème 1

Si L est un corps et H est un groupe fini du groupe des automorphismes de L , alors si $L^H = \{x \in L : \forall \sigma \in H, \sigma(x) = x\}$, L/L^H est une extension finie, $|H| = [L : L^H]$ et H est le groupe des L^H -automorphismes de L .

Démonstration. On note $m = [L : L^H]$ (éventuellement égal à ∞) et $n = |H|$. On va vérifier dans un premier temps que $m = n$.

- 1 Supposons que $m < n < +\infty$. Fixons x_1, \dots, x_m une base de L sur L^H et notons $H = \{\sigma_1, \dots, \sigma_n\}$. Considérons le système de m équations à n inconnues dans L , Y_1, \dots, Y_n défini par :

$$\forall j \in \llbracket 1, m \rrbracket, \sigma_1(x_j)Y_1 + \dots + \sigma_n(x_j)Y_n = 0$$

C'est un système surdéterminé donc il admet une solution non nulle (y_1, \dots, y_n) . Par suite, pour tout $x = \sum_{j=1}^m \alpha_j x_j \in L$, où $\alpha_j \in L^H$, on a

$$\sum_{i=1}^n \sigma_i(x)y_i = \sum_{i=1}^n \sum_{j=1}^m \alpha_j \sigma_i(x_j)y_i = \sum_{j=1}^m \alpha_j \left(\sum_{i=1}^n \sigma_i(x_j)y_i \right) = 0$$

On a donc $\sum_{i=1}^n y_i \sigma_i = 0$ avec les y_i non tous nuls ce qui contredit le lemme d'indépendance de Dedekind ci-dessous. Donc $m \geq n$.

- 2 Supposons que $m > n$. Il existe donc une famille (x_1, \dots, x_{n+1}) d'éléments de L libre sur L^H . Selon le même argument que pour le premier point, on peut trouver une famille non nulle $(y_1, \dots, y_{n+1}) \in L^{n+1}$ vérifiant (S) :

$$\forall i \in \llbracket 1, n \rrbracket, \sigma_i(x_1)y_1 + \dots + \sigma_i(x_{n+1})y_{n+1} = 0$$

Sans perte de généralité, on peut supposer que parmi toutes les solutions non nulles, (y_1, \dots, y_{n+1}) a un nombre minimal r de termes non nuls. Alors quitte à renuméroter, on peut supposer que $\forall i \leq r, y_i \neq 0$ et $\forall i > r, y_i = 0$. Ainsi, (S) se réécrit :

$$\forall i \in \llbracket 1, n \rrbracket, \sigma_i(x_1)y_1 + \dots + \sigma_i(x_r)y_r = 0$$

Soit $\sigma \in H$, appliquons σ au système (S) : $\forall i \in \llbracket 1, n \rrbracket, (\sigma \circ \sigma_i)(x_1)\sigma(y_1) + \dots + (\sigma \circ \sigma_i)\sigma(y_r) = 0$. Comme $\tau \mapsto \sigma \circ \tau$ est une permutation de l'ensemble fini H , on a donc (Δ) :

$$\forall i \in \llbracket 1, n \rrbracket, \sigma_i(x_1)y_1 + \dots + \sigma_i(x_r)y_r = 0$$

En multipliant (S) par $\sigma(y_1)$, (Δ) par y_1 et en additionnant les deux systèmes, on obtient

$$\forall i \in \llbracket 1, n \rrbracket, \sigma_i(x_2)(\sigma(y_1)y_2 - \sigma(y_2)y_1) + \dots + \sigma_i(x_r)(\sigma(y_1)y_r - \sigma(y_r)y_1) = 0$$

L'entier r étant le nombre minimal de termes non nuls d'une solution non triviale de (S) , on a $\forall j \in \llbracket 2, r \rrbracket, \sigma(y_1)y_j - y_1\sigma(y_j) = 0$, soit $\sigma(y_1y_j^{-1}) = y_1y_j^{-1}$ donc $\forall j \in \llbracket 2, r \rrbracket, y_1y_j^{-1} \in L^H$. Ainsi pour tout $2 \leq j \leq r$, il existe $z_j \in (L^H)^*$ tel que $y_j = z_j y_1$.

La ligne de (S) correspondant à $\sigma_i = \text{id}_L$ devient alors : $x_1y_1 + x_2z_2y_1 + \dots + x_rz_ry_1 = 0$ donc comme $y_1 \neq 0$, on a $x_1 + x_2z_2 + \dots + x_rz_r = 0$, de sorte que (x_1, \dots, x_r) est une famille liée, ce qui contredit l'hypothèse initiale. Donc $m \leq n < +\infty$ et finalement $m = n$.

- 3 Notons G le groupe des L^H -automorphismes de L . Il contient H de manière évidente. Montrons que G est fini. Soit (a_1, \dots, a_n) une base de L sur L^H , Π_1, \dots, Π_r les polynômes minimaux respectifs des a_i sur L^H et $f = \Pi_1 \dots \Pi_r \in L^H[X]$. Soit R l'ensemble (fini) des racines de f dans L . Comme $\Pi_j(a_j) = 0$ pour tout j , R contient $\{a_1, \dots, a_n\}$.

De plus, si $x = \sum_{i=1}^n \alpha_i a_i \in L$, où $\alpha_i \in L^H$, alors, pour tout élément σ de G , on a

$$\sigma(x) = \sum_{i=1}^n \alpha_i \sigma(a_i). \quad \text{Cela nous assure que } \begin{array}{l} \psi : G \longrightarrow \mathfrak{S}(R) \text{ est injective et donc} \\ \sigma \longmapsto \sigma|_R \end{array}$$

que G est fini.

On a $L^H \subset L^G \subset L$ par définition de G , et $L^G \subset L^H \subset L$ car $H \subset G$ donc $L^H = L^G$. Selon la conclusion du deuxième point, on a $|G| = [L : L^H] = [L : L^G] = |H|$ donc $G = H$.

□

Quelques précisions supplémentaires : ce développement s'inscrit dans une théorie plus générale, la théorie de Galois. Étant donné une extension de corps L/K , on s'intéresse à son groupe de Galois $\text{Gal}(L/K)$ qui est le groupe des K -automorphismes de corps de L . Le résultat majeur de cette théorie est la correspondance de Galois entre les corps intermédiaires $K \subset M \subset L$ et les sous-groupes H de $\text{Gal}(L/K)$:

Théorème 1

Si L/K est une extension galoisienne, les applications $\text{Fix} : H \mapsto L^H$ et $\text{Gal} : M \mapsto \text{Gal}(L/M)$ sont réciproques l'une de l'autre, où L^H , comme défini dans l'énoncé du théorème d'Artin est appelé sous-corps fixe de L associé à H

Il est remarquable qu'en vertu du théorème d'Artin, toute extension finie vérifie $\text{Gal} \circ \text{Fix} = \text{id}$.

Définition 1

Soit L/K une extension algébrique. On dit que c'est une extension galoisienne si $L^{\text{Gal}(L/K)} = K$.

On suppose à présent que K est un corps parfait, c'est-à-dire que si L/K est une extension algébrique, alors tout polynôme de $L[X]$ n'admet que des racines simples dans son corps de décomposition – L est dit *séparable*. La plupart des corps usuels sont parfaits : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, les corps finis. En revanche pour p premier, $\mathbb{F}_p(T)$ n'est pas parfait.

Définition 2

L'extension algébrique L/K est dite normale si tout polynôme irréductible $f \in K[X]$ admettant une racine dans L se décompose en produit de facteurs de degré 1 dans L .

Par exemple \mathbb{C}/\mathbb{R} est une extension normale.

Proposition 1

Soit L/K une extension finie, alors on a l'équivalence entre :

- 1 L/K est galoisienne ;
- 2 L/K est normale ;
- 3 L est le corps de décomposition d'un polynôme $f \in K[X]$;
- 4 $\text{Gal}(L/K)$ est d'ordre $[L : K]$;

En particulier si L/K est galoisienne finie et $K \subset M \subset L$ est un corps intermédiaire, alors L/M est galoisienne puisque L est le corps de décomposition de $f \in K[X] \subset M[X]$, ce qui prouve la correspondance de Galois.

Référence : *Invitation à l'algèbre : Théorie des groupes, des anneaux, des corps et des modules*, Alain Jeanneret, Daniel Lines, Editions Cépaduès, 2008. Voir également *Théorie algébrique des nombres* de Pierre Samuel aux éditions Hermann pour la théorie de Galois.



Méthodes itératives de résolution d'un système linéaire

Gabriel Lepetit, Antoine Diez

Soit $A \in \text{GL}_n(\mathbb{R})$, $b \in \mathbb{R}^n$. On étudie le système $Ax = b$.

Définition 1

Si $(M, N) \in \text{GL}_n(\mathbb{R}) \times \mathcal{M}_n(\mathbb{R})$ est tel que $A = M - N$, on dit que la méthode itérative associée à (M, N) converge si pour tout $u_0 \in \mathbb{R}^n$, la suite de premier terme u_0 et définie par $\forall k \in \mathbb{N}, u_{k+1} = M^{-1}(Nu_k + b)$ converge.

Théorème 1

La méthode itérative associée à (M, N) converge si et seulement si $\rho(M^{-1}N) < 1$

Commençons par montrer un lemme :

Lemme 1

Soit $A \in \mathcal{M}_n(\mathbb{C})$, $\varepsilon > 0$. Alors il existe une norme subordonnée $||| \cdot |||$ telle que $|||A||| \leq \rho(A) + \varepsilon$.

Démonstration. Comme A est à coefficients dans \mathbb{C} , elle est trigonalisable : on se donne donc P inversible et $T = (t_{ij})_{1 \leq i, j \leq n}$ triangulaire supérieure tels que $A = PTP^{-1}$.

Notons (e_1, \dots, e_n) la base canonique de \mathbb{C}^n . Pour $\delta > 0$, on pose $e'_1 = \delta^{-1}e_1$ et $D_\delta = \text{Diag}(1, \delta, \dots, \delta^{n-1})$.

On a donc $\forall j \in \llbracket 1, n \rrbracket, Te'_j = \delta^{j-1}Te_j = \delta^{j-1} \sum_{i=1}^j t_{ij}e_i = \sum_{i=1}^j \delta^{j-i}t_{ij}e'_i$, de sorte que $T_\delta =$

$$D_\delta^{-1}TD_\delta \text{ est la matrice } \begin{pmatrix} t_{11} & \delta t_{12} & \dots & \delta^{n-1}t_{1n} \\ & \ddots & \ddots & \dots \\ (0) & & \ddots & \delta t_{n-1n} \\ & & & t_{nn} \end{pmatrix}.$$

On définit pour $x \in \mathbb{R}^n$, $\|x\| = \|(PD_\delta)^{-1}x\|_\infty$, et on note $||| \cdot |||$ la norme subordonnée associée. On vérifie aisément que $\forall B \in \mathcal{M}_n(\mathbb{R}), |||B||| = |||(PD_\delta)^{-1}BPD_\delta|||_\infty$.

Or (admis ici), pour tout $B = (b_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{R})$, on a $|||B|||_\infty = \sup_{1 \leq i \leq n} \sum_{j=1}^n |b_{ij}|$. En choisissant $\delta > 0$ tel que pour tout $1 \leq i \leq n-1, \sum_{j=i+1}^n \delta^{j-i}|t_{ij}| \leq \varepsilon$, on obtient donc, puisque $\rho(A) = \sup_{1 \leq i \leq n} |t_{ii}|$, $|||A||| = |||T_\delta|||_\infty \leq \rho(A) + \varepsilon$. \square

Démonstration (du théorème). Soit $u \in \mathbb{R}^n$ tel que $Au = b$, c'est à dire $Mu = Nu + b$. Posons $e_k = u_k - u$ en reprenant les notations du théorème. Alors :

$$e_{k+1} = M^{-1}(Nu_k + b) - M^{-1}Nu - M^{-1}b = M^{-1}N(u_k - u) = M^{-1}Ne_k$$

Ainsi, par une récurrence immédiate, $\forall k \in \mathbb{N}, e_k = (M^{-1}N)^k e_0$. Dès lors, deux cas se présentent :

- Si $\rho(M^{-1}N) < 1$, on fixe $\varepsilon = \frac{1 - \rho(M^{-1}N)}{2}$ et le lemme nous fournit une norme subordonnée $\|\cdot\|$ telle que $\|M^{-1}N\| \leq \rho(M^{-1}N) + \varepsilon < 1$. Donc pour la norme $\|\cdot\|$ associée, on a pour tout k , $\|e_k\| \leq \|M^{-1}N\|^k \|e_0\|$ donc $\lim_{k \rightarrow +\infty} e_k = 0$ si bien que $(u_k)_k$ converge vers u .
- Si $\rho(M^{-1}N) \geq 1$, soit λ valeur propre complexe de module supérieur ou égal à 1, et $\tilde{u} = \tilde{u}_1 + i\tilde{u}_2$ un vecteur propre associé. Comme pour tout k , $(M^{-1}N)^k \tilde{u} = \lambda^k \tilde{u}$, la méthode itérative ne converge pas pour $u_0 = u + \tilde{u}_1$.

□

Décrivons maintenant quelques cas particuliers de méthodes itératives :

- Méthode de Jacobi : $M = \text{Diag}(a_{11}, \dots, a_{nn}) = D$ et $N = D - A$. On note $J = D^{-1}(D - A)$
- Méthode de Gauss-Seidel : $M = D - E$ où $D = \text{Diag}(a_{11}, \dots, a_{nn})$ et $E = -A_{\text{inf}}$, partie triangulaire inférieure stricte de A . $N = -A_{\text{sup}} = F$. On note $\mathcal{L}_1 = (D - E)^{-1}F$.
- Méthode de relaxation : $M = \frac{D}{\omega} - E$ et $N = \frac{1 - \omega}{\omega}D + F$, $\mathcal{L}_\omega = \left(\frac{D}{\omega} - E\right)^{-1} \left(\frac{1 - \omega}{\omega}D + F\right)$

Proposition 1

Si A est une matrice tridiagonale, $\rho(\mathcal{L}_1) = (\rho(J))^2$. La méthode de Gauss-Seidel a donc une vitesse de convergence double de celle de la méthode de Jacobi.

Démonstration. Remarque préliminaire : introduisons pour $\mu \neq 0$, $A(\mu) = \begin{pmatrix} b_1 & \mu^{-1}c_2 & & (0) \\ \mu a_2 & b_2 & \ddots & \\ & \ddots & \ddots & \mu^{-1}c_n \\ (0) & & \mu a_n & b_n \end{pmatrix}$,

où $A = A(1)$. Alors $A(\mu) = Q(\mu)A(1)Q(\mu)^{-1}$ où $Q(\mu) = \text{Diag}(\mu, \mu^2, \dots, \mu^{n-1})$, donc $\det A(\mu) = \det A(1)$.

Les valeurs propres de J sont les racines du polynôme caractéristique $p_J(\lambda) = \det(D^{-1}(E + F) - \lambda I)$, ce sont aussi celles de $q_J(\lambda) = \det(\lambda D - E - F)$. De même, les valeurs propres de \mathcal{L}_1 sont les racines de $p_{\mathcal{L}_1}(\lambda) = \det((D - E)^{-1}F - \lambda I)$, et celles de $q_{\mathcal{L}_1}(\lambda) = \det(\lambda D - \lambda E - F)$.

Mais selon la remarque préliminaire, pour tout $\lambda \in \mathbb{C}^*$, $q_{\mathcal{L}_1}(\lambda^2) = \det(\lambda^2 D - \lambda^2 E - F) = \lambda^n \det(\lambda D - \lambda E - \lambda^{-1}F) = \lambda^n \det(\lambda D - E - F) = \lambda^n q_J(\lambda)$.

Donc les valeurs propres non nulles de \mathcal{L}_1 sont les carrés de valeurs propres non nulles de J , ce qui permet de conclure. □

Proposition 2

Le rayon spectral de \mathcal{L}_ω est strictement supérieur à $|\omega - 1|$. La méthode de relaxation ne peut donc converger que si $\omega \in]0, 2[$.

Démonstration. La matrice $\mathcal{L}_\omega = \left(\frac{D}{\omega} - E\right)^{-1} \left(\frac{1 - \omega}{\omega}D + F\right)$ est trigonalisable comme produit de matrices trigonalisables et en notant $\lambda_1, \dots, \lambda_n$ ses valeurs propres avec multiplicité, on a

$$\prod_{i=1}^n \lambda_i = \det(\mathcal{L}_\omega) = \frac{\det\left(\frac{1 - \omega}{\omega}D + F\right)}{\det\left(\frac{D}{\omega} - E\right)} = \frac{\prod_{i=1}^n \frac{1 - \omega}{\omega} a_{ii}}{\prod_{i=1}^n \frac{a_{ii}}{\omega}} = (1 - \omega)^n$$

Donc $\rho(\mathcal{L}_\omega)^n \geq |\det(\mathcal{L}_\omega)| = |1 - \omega|^n$ de sorte que $\rho(\mathcal{L}_\omega) \geq |\omega - 1|$. □

Remarque. Par des techniques similaires, on montre que si A est tridiagonale et J a un spectre réel, la méthode de Jacobi et la méthode de relaxation pour $0 < \omega < 2$ convergent ou divergent simultanément. De plus, $\omega_0 = \frac{1}{1 + \sqrt{1 - \rho(J)^2}}$ est un paramètre de relaxation tel que $\rho(\mathcal{L}_{\omega_0})$ est minimal.

Référence : Ciarlet, Introduction à l'analyse numérique et à l'optimisation, p. 102

Errata

Titre 2 manquant un s

Def 7, Thm 8 : Ajouter $r < m$ et $s \in \{r+1, \dots, m\}$

Rem 11 une famille finie d'homomorphismes
de corps d'endomorphisme est toujours libre

$$\text{Thm 47 : } \|a_{r+1} - a_r\|_A^2 \leq (1 - \sigma_r) \|a_r - a\|_A^2$$