Institut Galilée
Université Sorbonne Paris Nord

NOTES DE COURS EN ALGÈBRE LINÉAIRE APPLIQUÉE

Version du 21 mars 2023

1. Méthodes effectives en algèbre linéaire

1.1. Réduction effective de Jordan.

Soit $\mathbb{K}$ un corps.

Théorème 1.1.1. *(Théorème de Jordan, version matricielle)*
Soit $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. On suppose χ_A scindé. Alors il existe une matrice P inversible et des blocs de Jordans associés aux valeurs propres de A telle que PAP^{-1} est diagonale par blocs, composée des blocs de Jordan sur la diagonale.

Remarque 1.1.2. Il y a de plus unicité à permutation près de ces blocs. La matrice inversible P peut être interprétée comme une matrice de changement de base (ordonnée), chaque $i$ème colonne donnant les coordonnées dans $\mathbb{K}^n$ du $i$ème vecteur de la nouvelle base (la base initiale étant la base canonique de $\mathbb{K}^n$).

Soit $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. On appelle f l'endomorphisme de $\mathbb{K}^n$ associé (relativement à la base canonique de $\mathbb{K}^n$).

Décrivons maintenant le procédé algorithmique pour obtenir la forme de Jordan de A, et une base associée.

Étape 1 : On calcule le polynôme caractéristique de A et on le factorise.

Ici on se heurte à plusieurs problèmes d'un point de vue effectif. Peut-on trouver les racines de χ_A de façon exacte et effective, de telle sorte qu'on peut l'écrire comme produit de $X - \lambda_i$? Pour rappel, la théorie de Galois nous dit que pour $n \geqslant 5$, il n'existe pas de procédé général pour déterminer les racines d'un polynôme de degré n.

Supposons pour la suite qu'on dispose de la factorisation

$$\chi_A = \prod_{i \in I} (X - \lambda_i)^{m_i},$$

avec les λ_i deux à deux distincts.

Étape 2 : Pour un i fixé, on cherche maintenant le nombre et la taille des blocs de Jordan pour la valeur propre λ_i.

On peut considérer le sous-espace caractéristique E_i associé à λ_i et l'endomorphisme restreint f_i de E_i. Celui-ci a (par construction) une unique valeur propre λ_i, et on peut donc poser $g = f_i - \lambda_i id_{E_i}$. Cet endomorphisme g est nilpotent, et on peut chercher la réduction de Jordan de g via la méthode algorithmique vue en tronc commun.

En pratique, sans passer explicitement par cet endomorphisme restreint, il suffit d'écrire la suite des noyaux itérés pour $g = f - \lambda_i id$ et de construire une base de E_i de la même façon que pour le cas nilpotent. La suite des noyaux itérés s'obtient par une recherche de noyaux, ce qui se fait algorithmiquement par un pivot sur les colonnes. Ce type de pivot permet à la fois de facilement trouver la dimension des noyaux qu'une base de chaque noyau. De plus, il est important de comprendre que pour un ordinateur, considérer des sous-espaces vectoriels se fait aisément en en donnant une base.

$$\{0\} \subset \ker(g) \subset \cdots \subset \ker(g^{d-1}) \subset \ker(g^d) = E_i.$$

Attention, il faut être capable de faire les calculs dans le pivot de façon exacte (corps finis ou rationnels, par exemple). Pour rappel, les matrices diagonalisables sont denses dans $M_n(\mathbb{C})$, ce qui signifie en pratique que modifier un coefficient d'un petit epsilon suffit

On rappelle que choisir un supplémentaire d'un sous-espace W d'un espace V revient à compléter une base de W en une base de V.

On utilise la version effective suivante du théorème de la base incomplète.

Lemme 1.1.3. *Soit W un sous-espace de V, avec des bases respectives $\mathcal{B}_W = \{w_1, \ldots, w_k\}$ et $\mathcal{B}_V = \{v_1, \ldots, v_k\}$.*

Alors il existe des vecteurs $v_{i_1}, \ldots, v_{i_{n-k}}$ tels que $\{w_1, \ldots, w_k, v_{i_1}, \ldots, v_{i_{n-k}}\}$ forme une base de V, c'est-à-dire $Vect(v_{i_1}, \ldots, v_{i_{n-k}})$ est un supplémentaire de W dans V.

L'algorithme de la Remarque 3.6 pages 36-37 du tronc commun est alors effectif. On obtient ainsi une base du sous-espace caractéristique E_i, adaptée à la décomposition de Jordan de $g = f - \lambda_i$.

Étape 3 : Il suffit maintenant de concaténer les bases obtenues à l'étape précédente pour les différentes valeurs de i. On obtient ainsi une base de Jordan pour la matrice A, dans le sens où en écrivant leurs coordonnées en colonnes on obtient la matrice P et où la matrice J s'obtient par blocs (en considérant la façon dont les vecteurs ont été obtenus dans la construction précédente, pour un certain λ_i).

Remarque 1.1.4. Le procédé revient au final à trouver des vecteurs engendrant des sous-espaces cycliques.

Exemple 1.1.5. On considère $C = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$ telle que $C^2 = \begin{pmatrix} 0 & 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

On a clairement $C^3 = 0$, donc la matrice est nilpotente d'indice 3. On peut écrire la suite des noyaux itérés, chercher algorithmiquement des bases de ces noyaux, puis appliquer l'algorithme effectif décrit précédemment.

Exemple 1.1.6. On considère $B = \begin{pmatrix} 4 & 3 & -2 \\ -3 & -1 & 3 \\ 2 & 3 & 0 \end{pmatrix}$ dont le polynôme caractéristique est $(X+1)(X-2)^2$.

Pour $\lambda = -1$, comme -1 est une racine simple la suite des noyaux itérés est triviale à écrire et est forcément de longueur minimale. Pour $\lambda = 2$, comme 2 est une racine double, on ne sait pas avant calcul la longueur de la suite des noyaux pour $f - 2id$.

Exemple 1.1.7. On considère $C = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & -2 & 2 & 3 \end{pmatrix}$ dont le polynôme caractéristique est $(X+1)^3(X-3)$.

1.2. **Algorithme effectif pour la décomposition de Dunford.** Soit $\mathbb{K}$ un corps de caractéristique nulle.

Théorème 1.2.1. *(Théorème de Dunford, version matricielle)*
Soit $n \in \mathbb{N}^*$ et $A \in M_n(\mathbb{K})$. On suppose χ_A scindé. Alors il existe une matrice D diagonalisable et une matrice N nilpotente telles que D et N commutent et que $A = N + D$.

On utilisera les lemmes suivants dans la preuve constructive de ce résultat :

Lemme 1.2.2. *Soit U matrice inversible et N matrice nilpotente commutant avec U.*
Alors $U - N$ est inversible.

Démonstration. (Preuve du lemme) On commence par traiter le cas $U = I_n$, où l'inverse de $I_n - N$ est la somme des N_i pour i entre 0 et l'indice de nilpotence de N. Le cas général se traite de façon similaire, en remarquant d'abord que $U - N = U(I_n - U^{-1}N)$ et que $U^{-1}N$ est encore nilpotente car U^{-1} et N commutent. □

Lemme 1.2.3. *Soit Q un polynôme de $\mathbb{K}[X]$.*
Alors il existe un polynôme $\tilde{Q} \in \mathbb{K}[X, Y]$ tel que

$$Q(X + Y) = Q(X) + YQ'(X) + Y^2\tilde{Q}(X, Y),$$

et il existe un polynôme $\hat{Q} \in \mathbb{K}[X, Y]$ tel que $Q(X + Y) = Q(X) + Y\hat{Q}(X, Y)$.

Démonstration. (Preuve du lemme) Par linéarité, il suffit de prouver le résultat pour $Q(X)$ de la forme X^k. La formule du binôme prouve le premier résultat, et le second se déduit du premier. □

Notons χ_A, qui est scincé, sous la forme $\prod(X - \lambda_i)^{n_i}$. Sans avoir besoin de connaitre les λ_i ni les n_i, il est possible de déterminer $P = \prod(X - \lambda_i)$ (du moins sur un corps de caractéristique nulle, ou si tous les n_i sont inférieurs à la caractéristique du corps). La clé est d'observer que $\prod(X - \lambda_i) = \dfrac{\chi_A}{pgcd(\chi_A, \chi'_A)}$. Le polynôme P est scindé à racines simples, donc s'il annule une matrice, celle-ci sera diagonalisable.

L'idée de la preuve du théorème est de montrer l'existence d'une suite de matrices (qui va stabiliser sur le D cherché) A_k définie par récurrence :

$A_0 = A$ et $A_{k+1} = A_k - P(A_k)P'(A_k)^{-1}$.

Un point crucial de la preuve sera que toutes les matrices en jeu sont des polynômes en A.

Soit alors H_k l'hypothèse de récurrence au rang k définie par :

H_k : La matrice A_k est définie et $P(A_k) = P(A)^{2^k}B_k$ avec B_k polynôme en A et $P'(A_k)$ inversible.

Pour l'Initialisation, il suffit de prouver que $P'(A_k)$ est inversible. Ceci se fait en remarquant que P et P' sont premiers entre eux, donc par le théorème de Bézout, il existe des polynômes U et V vérifiant $UP + VP' = 1$. En évaluant ceci en la matrice A, on trouve $V(A)P'(A) = I_n - U(A)P(A)$. Les hypothèses du lemme sont vérifiées et on trouve que $P'(A)$ est inversible.

Fixons maintenant $k \in \mathbb{N}$ tel que H_k est vraie.

La définition de la suite et H_k nous donnent l'existence de A_{k+1}.

Pour calculer $P(A_{k+1}$, par hypothèse de récurrence, on applique le second lemme avec $Q = P$, $X = A_k$ et $Y = -P(A_k)P'(A_k)^{-1}$. Ceci fait apparaitre $P(A_k) - P(A_k)$ et un terme qui après calcul peut s'écrire sous la forme $P(A)^{2^{k+1}}$ fois un polynôme en A.

Pour montrer l'inversibilité de $P'(A_{k+1})$, on utilise la seconde partie du deuxième lemme, pour $Q = P'$ et les mêmes X et Y que précédemment. On obtient $P'(A_{k+1}) = P'(A_k) +$

$P(A_k)C_k$ où $P'(A_k)$ est inversible par hypthèse de récurrence, où $P(A_k)$ est nilpotent (par Cayley-Hamilton) et où C_k est un polynôme en A. Le premier lemme donne donc que $P'(A_{k+1})$ est inversible.

Ceci prouve H_{k+1}, et par suite, notamment que la suite A_k est bien définie.

Il reste à montrer qu'elle stabilise et que la valeur limite est diagonalisable.

Pour $r = \max n_i$, le polynôme P^r est un multiple de χ_A, et donc par le théorème de Cayley-Hamilton, $P^r(A)$ est nul. La formule exprimant $P(A_k)$ en fonction de $P(A)$ (2e partie de H_k) donne alors à la fois que la suite des A_k stabilise (pour k vérifiant $2^k \geqslant r$) (appelons D la valeur limite de cette suite de matrices) et que $P(D)$ est nul, ce qui implique que D est diagonalisable.

On pose ensuite $N = A - D$. On peut écrire N comme une somme télescopique finie de $A_{k+1} - A_k$, qui sont des matrices nilpotentes commutant 2 à 2 (car toutes sont des polynômes en A). Une telle somme est encore nilpotente.

À nouveau par un argument de polynômes en A, les matrices D et N commutent.

Ceci prouve le théorème.

1.3. **Recherche de polynôme minimal.** Soit A dans $M_n(\mathbb{K})$.

L'idée est de déterminer μ_A en étudiant successivement la liberté des familles $\{Id, A\}$ puis $\{Id, A, A^2\}$, jusqu'à la première famille $\{Id, A, \ldots, A^k\}$ liée (donc k est minimal en ce sens). Une relation de liaison $\sum_i \lambda_i A^i$ aura alors forcément un coefficient a_k non nul (par minimalité de k). Et en divisant par a_k, on obtient ainsi les coefficients du polynôme unitaire de plus petit degré (à nouveau car k est minimal) s'annulant sur la matrice A.

En pratique, pour utiliser des algorithmes déjà programmés cherchant le noyau (donc liberté ou relation de liaison) sur une famille de vecteurs colonnes, il est utile de fixer un isomorphisme entre $M_n(K)$ et K^{n^2}. Ceci revient à fixer un "ordre de lecture" sur les coefficients d'une matrice.

On sait que cet algorithme est terminant car le degré du polynôme minimal est inférieur à n (et même sans ce résultat, dans un espace de dimension n^2, toute famille de plus de n^2 vecteurs est liée).

Exemple 1.3.1. Pour la matrice $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on peut associer le vecteur colonne $(1, 1, 0, 1)$ (en lisant ligne par ligne). L'identité se lit $(1, 0, 0, 1)$. Et A^2 se lit $(1, 2, 0, 1)$.

La famille $\{Id, A\}$ est libre, mais la famille $\{Id, A, A^2\}$ est liée. On trouve (par un algorithme du pivot sur les colonnes) une combinaison de la forme $A^2 - 2A + Id = 0$, ce qui donne donc $\mu_A = X^2 - 2X + 1$.

1.4. **Décomposition de Bruhat.**

Théorème 1.4.1. *Soit $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Notons T_U l'ensemble des matrices triangulaires supérieures inversibles, et pour $\sigma \in S_n$, notons P_n la matrice de permutation associée à σ.*

Alors $GL_n(\mathbb{K}) = \bigcup_{\sigma \in S_n} T_U P_n T_U$. De plus cette union est disjointe.

Démonstration. La preuve de l'existence se fait algorithmiquement. On fixe A dans $Gl_n(\mathbb{K})$ et on prouve qu'il existe T_1, T_2 et σ tels que $A = T_1 P_\sigma T_2$.

La preuve de l'existence se fait en supposant l'existence de telles écritures, et on montre l'unicité de la permutation associée (les matrices triangulaires ne sont pas uniques). □

1.5. **Révisions sur les corps finis.**

1.5.a. -. Soit P le polynôme $X^2 + X + 1$ sur $\mathbb{F}_2[X]$.

1) Quelle est la dimension (comme $\mathbb{F}_2$-espace vectoriel) de $\mathbb{F}_2[X]/(P)$? En donner une base simple.

2) Ecrire la table de multiplication de $\mathbb{F}_4 = \mathbb{F}_2[X]/(P)$ et montrer que $(\mathbb{F}_4^\times, \times) \simeq \langle \overline{X} \rangle$ (iso de groupes).

1.5.b. -. Soit $\mathbb{K}$ un corps et p sa caractéristique.
a) Montrer que $\mathbb{K}$ a une structure de $\mathbb{F}_p$-espace vectoriel.
b) En déduire que si $\mathbb{K}$ est fini, il existe $n \in \mathbb{N}^*$ tel que $|\mathbb{K}| = p^n$.

1.5.c. -. Soit A un anneau (commutatif unitaire) intègre de caractéristique p.
On considère l'application $Frob : A \to A$ définie par $Frob(x) = x^p$.

a) Montrer que $Frob$ est un endomorphisme d'anneaux unitaires.
b) Pour $A = \mathbb{F}_p$, montrer que $Frob = id$.
c) Sur $\mathbb{F}_p[X]$, montrer que $Frob$ est linéaire et déterminer ses points fixes.

1.5.d. -. Factoriser $X^p - X \in \mathbb{F}_p[X]$. En déduire les points fixes de $Frob$ sur $\mathbb{F}_q$, où $q = p^n$.

1.5.e. -. Montrer que $\mathbb{F}_2[X]/(X^3 + X + 1)$ et $\mathbb{F}_2[X]/(X^4 + X + 1)$ définissent $\mathbb{F}_8$ et $\mathbb{F}_{16}$. Donner un générateur du groupe multiplicatif de ces corps.

On rappelle pour la suite du cours le théorème fondamental suivant :
Pour tout nombre premier p, pour tout entier naturel non nul n, il existe un corps de cardinal p^n. Ces corps s'obtiennent par exemple comme quotient de $\mathbb{F}_p[X]$ par un polynôme irréductible (engendrant un idéal maximal).

1.6. **Factorisation de polynômes : algorithme de Berlekamp.**

2. Codes correcteurs