Anaël Marit ENS Rennes

RÉDUCTION DE FROBENIUS

- [148, 150, 151, 159] –

—

Dans ce développement, on va démontrer la classique théorème de réduction de Frobenius. Il s'agit d'un résultat qui a d'importantes conséquences théoriques et qui répond au problème de classifier toutes les orbites de matrices sous l'action de similitude du groupe linéaire, sans aucune hypothèse sur le corps de base. On commencera par introduire la forme de Frobenius, les invariants de similitude dont on démontrera l'existence et l'unicité, et on terminera par une application intéressante qu'on peut faire de ce résultat.

Remarquez que le développement est **extrêmement** *long. Je pense que vous pouvez traiter uniquement l'existence à l'oral ou alors l'unicité et l'application selon la leçon présentée et/ou vos affinités, mais que tout faire est déraisonnable.*

Soient K un corps quelconque [(i)] et n un entier naturel non-nul. Etant donné un polynôme $P \in K[X]$ de degré n unitaire, qu'on note sous forme développée :

$$P = X^n + \sum_{i=0}^{n-1} a_i X^i \tag{1}$$

on note sa matrice compagnon :

$$C_P := \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix} \tag{2}$$

Etant donné u un endomorphisme d'un K-espace vectoriel de dimension finie, on notera π_u son polynôme minimal. Si de plus x est un vecteur de l'espace sous-jacent, on note $\pi_{u,x}$ le polynôme minimal de u en x, c'est-à-dire l'unique générateur unitaire de l'idéal :

$$\{P \in K[X] \mid P(u)(x) = 0\} \tag{3}$$

(i). Dans eertains livres, comme le Rombaldi, le théorème de Frobenius suppose que le corps K est infini. Cette hypothèse intervient pour la preuve d'un lemme qui est fondamental pour le développement : pour $u \in \mathscr{L}(E)$, il existe un vecteur $x \in E$ tel que le polynôme minimal en x de u soit égal au polynôme minimal. Certains auteurs supposent le corps K infini car la preuve est alors quasi immédiate, mais ce résultat reste vrai avec K quelconque. J'ai mis en annexe une preuve qui fonctionne dans le cas général.

Théorème 1 (Frobenius ([1], théorème B.2.1)). *Soit E un K-espace vectoriel de dimension n et soit $u \in \mathscr{L}(E)$. Il existe une suite $(E_1, \dots, E_r)$ de sous-espaces vectoriels de E tels que :*

1. $E = \bigoplus_{i=1}^{r} E_i$
2. *u stabilise chacun des E_i et y induit un endomorphisme cyclique.*
3. *La suite $(P_1, \dots, P_r)$ des polynômes minimaux des endomorphismes induits sur les (E_i) est telle que $P_r | \dots | P_1$*

De plus, la suite de polynômes (P_i) ainsi définis est unique : on l'appelle suite des invariants de similitudes *de u.*

Le théorème de Frobenius répond effectivement au problème de classification des orbites de similitude de $\mathbb{M}_n(K)$:

Corollaire 2. *Deux matrices de $\mathbb{M}_n(K)$ sont semblables si, et seulement si, elles ont les mêmes invariants de similitude.*

Existence de la forme de Frobenius

On raisonne par récurrence sur n.

Pour $n = 1$, le résultat est évident : on prend $r = 1$, $E_1 = E$ et on a $P_1 = X - u(1)$ en assimilant E à K.

Supposons le résultat acquis si la dimension de E est inférieure stricte à n. Dans ce cas, soit $x \in E \setminus \{0\}$ tel que $\pi_{u,x} = \pi_u$. On pose E_1 l'espace cyclique engendré par u et x, c'est-à-dire :

$$E_1 := \mathrm{Vect}(u^k(x) \mid k \in \mathbb{N}) \tag{4}$$

Tout l'enjeu du développement est de trouver un supplémentaire de E_1 stable par u pour pouvoir y appliquer l'hypothèse de récurrence. Pour cela, on raisonne par dualité. Soit $(e_1, \dots, e_p)$ la base de E_1 formée des $e_i := u^{i-1}(x)$ avec p le degré du polynôme minimal en x de u. On la complète en une base de E. Notons (e_i^*) la base duale ainsi obtenue. On considère alors le sous-espace de E^* :

$$G := \mathrm{Vect}((u^T)^k(e_p^*) \mid 0 \leqslant k \leqslant p-1) \tag{5}$$

G est stable par u^T. En effet, pour $0 \leqslant k < p-1$, on a :

$$u^T((u^T)^k(e_p^*)) = (e^T)^{k-1}(e_p^*) \in G \tag{6}$$

et pour $k = p-1$, on utilise le fait que $\pi_u(u) = 0$ et p est le degré de π_u, donc u^p est une combinaison linéaire des $(u^k)_{0 \leqslant k \leqslant p-1}$. Il en découle immédiatement que $u^T((u^T)^{p-1}(e_p^*)) \in G$.

Par ailleurs, G est de dimenion p. En effet, soient $(\lambda_1, \dots, \lambda_p)$ des scalaires tels que :

$$\sum_{k=1}^{p} \lambda_k (u^T)^{k-1}(e_p^*) = 0 \tag{7}$$

Par l'absurde, on suppose que les (λ_i) ne sont pas tous nuls et on note r le plus grand indice tel que $\lambda_r \neq 0$. Alors :

$$0 = \left[\sum_{k=1}^{r} \lambda_k (u^T)^{k-1}(e_p^*)\right](u^{p-r}(x)) \tag{8}$$

$$= e_p^*(\lambda_r \underbrace{u^{p-1}(x)}_{=:e_p}) + \underbrace{e_p^*\left(\sum_{k=1}^{r-1}(\lambda_k(u^{k+p-r-1}(x))\right)}_{=0 \text{ car } k+p-r-1<p-1} \tag{9}$$

$$= \lambda_r \tag{10}$$

ce qui fournit une contradiction. Remarquons au passage qu'on a montré que pour tout $k \in [\![0, p-1]\!]$,

L'annulateur de G, qu'on note G°, est donc un sous-espace de E de dimension $n-p$, stable par u. Montrons que c'est un supplémentaire de F. Par relation sur les dimensions, il suffit de montrer que leur intersection est réduite à $\{0\}$. Soit $z \in F \subset G\circ$. On décompose z sous la forme :

$$z = \sum_{k=1}^{p} \lambda_k u^{k-1}(x) \tag{11}$$

et on suppose par l'absurde que z est non nul. En prenant encore une fois r le plus grand indice tel que $\lambda_r \neq 0$ et en appliquant $(u^T)^{p-r-1}(e_p^*) \in G$ à z, on obtient :

$$0 = \lambda_r \text{ (ii)} \tag{12}$$

Ainsi, on peut appliquer l'hypothèse de récurrence à l'endomorphisme induit sur G° : il existe une suite $(E_2, \ldots, E_r)$ de sous-espaces vectoriels de G° telle que $G^\circ = \bigoplus_{i=2}^{r} E_i$ et telle que les polynôme minimaux des endomorphismes induits (qu'on appelle (P_i)) satisfont les bonnes relations de divisibilité.

Attention, la preuve n'est pas encore terminée ! En effet, il n'y a a priori aucune raison pour que $P_2|P_1$. Pour obtenir cette dernière relation, il faut remarquer que $P_1 = \pi_{u,x}$, qui par construction est le polynôme minimal de u. Donc $P_1(u_{|E_2}) = 0$ et puisque P_2 est le polynôme minimal de $u_{|E_2}$, on a bien $P_2|P_1$.

Unicité des facteurs invariants

Le raisonnement est classique : on se donne $(F_1, \ldots, F_r)$ et $(G_1, \ldots, G_s)$ deux suites de sous-espaces vectoriels comme dans le théorème, et on note $(P_1, \ldots, P_r)$ et $(Q_1, \ldots, Q_s)$ les polynômes minimaux des endomorphismes induits. On note de plus, pour alléger la suite, $(v_1, \ldots, v_r)$ et $(w_1, \ldots, w_s)$ les endomorphismes induits sur ces espaces. Par l'absurde, on suppose que les suites (P_i) et (Q_j) sont distinctes et on note i_0 l'indice minimal tel que $P_{i_0} \neq Q_{i_0}$ (iii). Comme les (F_i)

(ii). Moi aussi ça m'embête de faire deux fois exactement la même preuve mais je n'ai malheureusement pas trouvé de moyen simple pour expliquer pourquoi cette deuxième preuve découle immédiatement de notre travail précédent.

(iii). qui existe même si $r \neq s$ car $\sum_{i=1}^{r} \deg(P_i) = \sum_{j=1}^{s} \deg(Q_j) = n$ donc si $r < s$ et les (P_i) sont les r-premiers (Q_j), par égalité sur les degrés, les (Q_j) restants sont des constantes non nulles, ce qui est absurde car ce sont des polynômes minimaux.

et les (G_j) sont stables par u, ils sont stables par tout polynôme en u. En particulier :

$$P_{i_0}(u)(E) = \bigoplus_{i=1}^{r} P_{i_0}(u)(E_i) = \bigoplus_{j=1}^{s} P_{i_0}(u)(F_j) \tag{13}$$

et comme, pour $i, j > i_0$, les polynômes minimaux des endomorphismes induits par u sur E_i et F_j divisent P_{i_0}, on a :

$$\forall i, j > i_0,\ \{0\} = P_{i_0}(E_i) = P_{i_0}(F_j) \tag{$\star$}$$

et cette égalité reste vraie pour $i = i_0$. Ainsi :

$$P_{i_0}(u)(E) = \bigoplus_{i=1}^{i_0-1} P_{i_0}(u)(E_i) = P_{i_0}(G_{i_0}) \oplus \bigoplus_{j=1}^{i_0-1} P_{i_0}(u)(F_j) \tag{14}$$

Utilisons maintenant le fait que les (v_i) et les (w_j) sont cycliques : ils sont donc représentés dans une certaine base par la matrice compagnon de leurs polynômes minimaux respectifs. En particulier, pour $i < i_0$, v_i et w_i sont représentés par une même matrice ; de même donc pour $P_{i_0}(v_i)$ et $P_{i_0}(w_i)$. Ceci implique que ces endomorphismes ont même rang, et donc on a :

$$\forall i < i_0,\ \dim(P_{i_0}(u)(F_i)) = \dim(P_{i_0}(u)(G_i)) \tag{15}$$

On passe alors à la dimension dans $(\star)$ et on montre :

$$\dim(P_{i_0}(u)(G_{i_0}) = \cdots = \dim(P_{i_0}(u)(G_s) = 0 \tag{16}$$

et donc P_{i_0} annule w_{i_0}, ce qui implique qu'il est divisé par son polynôme minimal Q_{i_0}.

Le raisonnement étant symétrique en les (P_i) et les (Q_j), on obtient de même que $P_{i_0} | Q_{i_0}$ et donc ces polynômes sont égaux, ce qui prouve l'unicité des invariants de similitude !

Réponse au problème de classification

On va maintenant démontrer le corollaire, bien que je pense que cette partie puisse être passée à l'oral si vous regardez bien le jury dans les yeux, parce qu'elle se résume franchement à un jeu d'écriture.

Soient A et B dans $\mathbb{M}_n(K)$. Le théorème de Frobénius affirme qu'il existe des bases $\mathscr{B}_1$ et $\mathscr{B}_2$ de K^n dans lesquelles les matrices des endomorphismes canoniquement associés à A et B sont :

$$\begin{pmatrix} C_{P_1} & 0 & 0 & \dots & 0 \\ 0 & C_{P_2} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & C_{P_r} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} C_{Q_1} & 0 & 0 & \dots & 0 \\ 0 & C_{Q_2} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & C_{Q_s} \end{pmatrix} \tag{17}$$

où les (P_i) et (Q_j) sont les invariants de similitude respectifs de A et de B. Il est donc clair que si A et B sont semblables si, et seulement si, elles ont les mêmes invariants.

Une application

Une conséquence théorique intéressante de ce résultat est la suivante :

Proposition 3. *Soit L/K une extension de corps et soit A et B deux matrices carrées de taille n à coefficients dans K. Les assertions suivantes sont équivalentes :*

1. *A et B sont K-semblables.*
2. *A et B sont L-semblables.*

Démonstration. Supposons qu'il existe P une matrice carrée inversible à coefficients dans L telle que $P^{-1}AP = B$. Ceci implique que A et B ont les mêmes invariants de similitude en tant que matrices de $\mathbb{M}_n(L)$. Mais les invariants de similitude à coefficients dans K satisfont les hypothèses du théorème de Frobenius lorsqu'on plonge A et B dans $\mathbb{M}_n(L)$: par unicité, les invariants de similitude de A et B vues comme éléments de $\mathbb{M}_n(K)$ sont identiques, et donc A et B sont semblables dans $\mathbb{M}_n(K)$. □

Annexe

Comme je l'indiquais plus haut, certains livres supposent le corps K infini pour faciliter la preuve d'un lemme qu'on a utilisé plus haut. Afin que la preuve soit complète, j'ajoute une démonstration de ce lemme dans le cas général, car je pense qu'il est important de la connaître si on veut traiter le théorème de Frobenius dans toute sa généralité.

Lemme 4 ([1], chapitre IV, paragraphe 2, exercice 3). *Soit $u \in \mathscr{L}(E)$. Il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$.*

Démonstration. Etudions d'abord le cas où π_u est une puissance d'un polynôme irréductible dans $K[X]$, qu'on note P. On a alors $\pi_u = P^\alpha$. Comme on a toujours, pour tout $x \in E$, $\pi_{u,x} | \pi_u$, il existe un entier $\beta(x)$ tel que $\pi_{u,x} = P^{\beta(x)}$. Il est alors assez immédiat de remarquer :

$$\alpha = \max_{x \in E} \beta(x) \tag{18}$$

où le maximum est justifié car β est à valeurs dans une partie finie de $\mathbb{N}$. Donc il existe x tel que $\beta(x) = \alpha$, c'est-à-dire tel que $\pi_{u,x} = \pi_u$.

Dans le cas général, décomposons π_u en produit d'irréductibles :

$$\pi_u = \prod_{i=1}^{r} P_i^{\alpha_i} \tag{19}$$

On utilise alors le lemme des noyaux et le fait que $\pi_u(u) = 0$:

$$E = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_i^{\alpha_i}(u)) \tag{20}$$

Pour $i \in [\![1, r]\!]$, notons u_i l'endomorphisme induit sur $\mathrm{Ker}(P_i^{\alpha_i}(u))$. On montre facilement que le polynôme minimal de u_i est $P_i^{\alpha_i}$, donc on se rammène au cas précédent. Il existe donc $x_i \in \mathrm{Ker}(P_i^{\alpha_i}(u))$ tel que $\pi_{u_i,x_i} = \pi_{u_i}$.

On pose alors $x = x_1 + \cdots + x_r$. On a alors, pour $Q \in K[X]$:

$$Q(u)(x) = 0 \iff \sum_{i=1}^{r} Q(u_i)(x_i) = 0 \tag{21}$$

$$\iff \forall i \in [\![1, r]\!],\ Q(u_i)(x_i) = 0 \text{ (iv)} \tag{22}$$

$$\iff \forall i \in [\![1, r]\!],\ P_i^{\alpha_i} | Q \tag{23}$$

$$\iff \pi_u | Q \tag{24}$$

ce qui prouve que $\pi_{u,x} = \pi_u$. □

Le mot de la fin

Quelques remarques peut-être sur ce développement !

- *Il s'agit d'un résultat de réduction qui fournit une "forme normale" pour n'importe quelle matrice. Malheureusement, la forme de Frobenius a le mauvais goût de ne pas coïncider avec les autres formes normales lorsque celles-ci existent. Par exemple, si A est diagonalisable, sa forme de Frobenius peut ne pas être diagonale, et la diagonalisabilité ne se lit pas directement sur la forme de Frobenius (contrairement à la forme de Jordan).*
- *En contrepartie, la forme de Frobenius se calcule explicitement via un algorithme. Je ne sais pas s'il est à connâitre, mais a priori le jury peut demander des calculs explicites de facteurs invariants, d'après ce que j'ai pu lire à droite à gauche. L'algo général est celui qui permet de calculer la forme de Smith d'une matrice à coefficients dans un anneau euclidien. A ce propos...*
- *...peut-être aurez-vous remarqué une étonnante similitude entre ce théorème et le théorème de structure des groupes abéliens finis (il existe une unique suite d'entiers $d_r | \ldots | d_1$, etc.) : ce n'est pas un hasard ! Ces deux théorèmes sont en fait des cas particuliers du théorème de structure des modules de type fini sur un anneau principal, qu'on peut voir comme corollaire de la forme de Smith des matrices à coefficients dans un anneau principal. Bien sûr, tout ceci est hors-programme à l'agreg, mais si ce point de vue vous intéresse (et c'est bien normal !), je trouve que le polycopié de Matoumatheux à ce sujet est une bonne première approche qui reste proche en un sens de l'agreg, et dans lequel se trouvent de plus amples références : [2].*

Références

[1] Xavier Gourdon. *Algèbre et probabilités*. Ellipses.

[2] Matthias Hostein. *La réduction par la théorie des modules*. 2024. URL : `https://perso.eleves.ens-rennes.fr/people/matthias.hostein/Fichiers_site/La_reduction_par_la_theorie_des_modules.pdf`.

(iv). Car $Q(u)$ stabilise la somme directe en espaces caractéristiques.