Réduction de Frobenius

Perrine Jouteur

Ce développement est très pratique car il peut se recaser dans beaucoup de leçons : 101, 122, 151, 153, 154, 155, 159. Cette version se réfère au livre *Nouvelles histoires hédonistes de groupes et de géométries* de Caldero et Germoni. Comme la totalité de ce qui suit ne peut pas se présenter en quinze minutes (à moins d'être doué de pouvoirs supersoniques), je conseille de présenter seulement l'existence des invariants de similitude, et de choisir un ou deux lemmes à démontrer, le reste étant admis.

Soit k un corps, E un k-espace vectoriel de dimension finie n, et u un endomorphisme de E.

1 Des lemmes

Lemme 1.1 Pour tout $x \in E$, il existe un unique polynôme unitaire $\pi_{u,x}$ générateur de l'idéal

$$\{P \in k[X] \mid P(u)(x) = 0\}.$$

En particulier, $\pi_{u,x} | \pi_u$, et le degré de $\pi_{u,x}$ est la dimension du sous-espace cyclique $k[u] \cdot x$.

Démonstration
Il suffit simplement de voir que l'anneau $k[X]$ est principal.
Petite remarque tout de même, concernant le cas où $x = 0$. Dans ce cas, l'idéal est l'ensemble des polynômes, $k[X]$, et donc on prend $\pi_{u,x} = 1$. ■

Lemme 1.2 Il existe $x \in E$ tel que $\pi_{u,x} = \pi_u$.

Démonstration
On décompose π_u en polynômes irréductibles sur k : $\pi_u = \prod_{i=1}^{r} P_i^{\alpha_i}$.

Posons $K_i = \mathrm{Ker}(P_i^{\alpha_i}(u))$. Alors K_i est un sous-espace stable par u, et par lemme des noyaux on a $E = \bigoplus_{i=1}^{r} K_i$. De plus, l'endomorphisme induit u_i par u sur K_i vérifie $\pi_{u_i} = P_i^{\alpha_i}$.
Supposons que pour tout $x_i \in K_i$, le polynôme π_{u_i,x_i} divise strictement $P_i^{\alpha_i}$, c'est-à-dire divise $P_i^{\alpha_i - 1}$. Alors pour tout $x_i \in K_i$, $P_i^{\alpha_i - 1}(u_i)(x_i) = 0$, et donc l'endomorphisme $P_i^{\alpha_i - 1}(u_i)$ est nul sur K_i, ce qui est absurde puisque $P_i^{\alpha_i}$ était le polynôme minimal de u_i sur K_i.
Ainsi il existe $x_i \in K_i$ tel que $\pi_{u_i,x_i} = P_i^{\alpha_i}$.

Soit maintenant $x = x_1 + \cdots + x_r$. Montrons que $\pi_u = \pi_{u,x}$.
On a déjà la divisibilité $\pi_{u,x} | \pi_u$. Il suffit donc de montrer que $\pi_u | \pi_{u,x}$. Montrons donc que $\pi_{u,x}(u) = 0$.
Soit $y \in E$. On le décompose en $y = y_1 + \cdots + y_r$ avec $y_i \in K_i$. Alors

$$\pi_{u,x}(u)(y) = \pi_{u,x}(u)(y_1) + \cdots + \pi_{u,x}(u)(y_r).$$

Or pour tout $i \in [\![1, r]\!]$,

$$\pi_{u,x}(u)(y_i) = \pi_{u,x}(u_i)(y_i) = \left(\prod_{j=1}^{r} P_j^{\alpha_j} \right)(u_i)(y_i) = \left(\prod_{j \neq i}^{r} P_j^{\alpha_j} \right)(u_i) \circ P_i^{\alpha_i}(u_i)(y_i) = 0.$$

D'où $\pi_{u,x}(u)(y) = 0$, et donc $\pi_u = \pi_{u,x}$. ■

Lemme 1.3 Le polynôme caractéristique d'une matrice compagnon C_P est P.

Démonstration
C'est un résultat classique, on pourra trouver une démonstration dans le livre d'Algèbre de Gourdon. ■

Lemme 1.4 Il y a équivalence entre

(i) E est u-cyclique ;

(ii) il existe une base de E telle que la matrice de u soit une matrice compagnon ;

(iii) $\pi_u = \chi_u$;

(iv) $\deg(\pi_u) = \dim(E)$.

Démonstration
Il suffit de l'écrire, en utilisant le lemme 1.2 pour l'implication $(iii) \Rightarrow (ii)$. ■

Lemme 1.5 Soit x tel que $\pi_{u,x} = \pi_u$. Alors $k[u](x)$ possède un supplémentaire u-stable.

Démonstration
Notons d le degré de π_u. Le vecteur x fournit une base $(x, u(x), \cdots, u^{d-1}(x))$ de $k[u](x)$.
Soit ϕ une forme linéaire telle que

$$\phi(x) = \phi(u(x)) = \cdots = \phi(u^{d-2}(x)) = 0 \text{ et } \phi(u^{d-1}(x)) = 1.$$

Alors la famille $(\phi, \phi \circ u, \cdots, \phi \circ u^{d-1})$ est libre (ça se vérifie simplement). Notons G le sous-espace de E^* engendré par cette famille, et $F = G^\perp \subset E$. Montrons que F est un supplémentaire u-stable de $k[u](x)$.

Le fait que F soit u-stable est immédiat, par construction de G.
Le fait que $F \cap k[u](x) = 0$ vient aussi naturellement quand on écrit les choses proprement.
Enfin, comme $k[u](x)$ est de dimension d et F de dimension $n - d$, on a que F est un supplémentaire de $k[u](x)$ qui est u-stable. ■

2 Le théorème

Théorème 2.1 On suppose ici que E n'est pas réduit à l'espace nul.
Il existe un unique $r > 0$, et une unique famille de polynômes unitaires non constants $(P_1, \cdots, P_r)$ tels qu'il existe une famille de vecteurs $(x_1, \cdots, x_r)$ vérifiant :

(i) $P_r | P_{s-1} | \cdots | P_1$,

(ii) $E = \bigoplus_{k=1}^{r} k[u] \cdot x_k$ où $\pi_{u,x_k} = P_k$.

Démonstration
• **Existence** : par récurrence.
◦ Initialisation : prenons $n = 1$. Soit $E = k$ et u un endomorphisme de E que l'on assimile à un scalaire $\lambda \in k$. Soit $x_1 = 1 \in E$, et $P_1 = X - \lambda$. Alors P_1 est le polynôme minimal de u, et on a $\pi_{u,1} = P_1$. De plus, $k[u](1) = k = E$ et donc on a ce qu'on voulait.

◦ Hérédité : supposons le résultat vrai pour tout espace de dimension strictement plus petite que n, et pour tout endomorphisme. Soit E un espace de dimension n et u un endomorphisme de E. D'après le lemme 1.2, il existe un vecteur x_1 de E tel que $\pi_{u,x_1} = \pi_u$. Posons alors $P_1 = \pi_u$. D'après le lemme 1.5, il existe un supplémentaire u-stable à $k[u](x_1)$. Notons F un tel supplémentaire. Alors $E = k[u](x_1) \oplus F$, et F est de dimension strictement inférieure à n puisque π_u est de degré plus grand que 1. On peut alors appliquer l'hypothèse de récurrence à l'espace F et à l'endomorphisme induit par u sur F : il existe des polynômes $\tilde{P_1}, \cdots, \tilde{P_s}$ et des vecteurs de F, $(\tilde{x_1}, \cdots, \tilde{x_s})$ tels qu'on ait $\tilde{P_s} | \cdots | \tilde{P_1}$ et $F = \bigoplus_{j=1}^{s} k[u_{|F}](\tilde{x_j})$, avec $\pi_{u_{|F},\tilde{x_j}} = \tilde{P_j}$.
Or pour tout j, comme F est stable par u et que $\tilde{x_j} \in F$, on a $k[u_{|F}](\tilde{x_j}) = k[u](\tilde{x_j})$ et $\pi_{u_{|F},\tilde{x_j}} = \pi_{u,\tilde{x_j}}$.
Donc il suffit de poser $r = s + 1$, $P_2, \cdots, P_r = \tilde{P_1}, \cdots, \tilde{P_s}$ et $x_2, \cdots, x_r = \tilde{x_1}, \cdots, \tilde{x_s}$, et on a

$$E = k[u](x_1) \oplus F = k[u](x_1) \oplus \bigoplus_{i=2}^{r} k[u](x_i).$$

Avec $\pi_{u,x_i} = P_i$ pour tout i. Il reste seulement à vérifier que P_2 divise P_1, et cela vient du fait que $P_2 = \pi_{u,x_2} | \pi_u = P_1$.

• **Unicité** : soient $r > 0$, $s > 0$, deux entiers, soient deux familles de polynômes $(P_1, \cdots, P_r)$ et $(Q_1, \cdots, Q_s)$ et des vecteurs $(x_1, \cdots, x_r)$ et $(y_1, \cdots, y_s)$ qui conviennent.

Montrons d'abord que $P_1 = Q_1 = \pi_u$. On le montre pour P_1, et on aura le même raisonnement pour Q_1. Comme $P_1 = \pi_{u,x_1}$, on a déjà la divisibilité $P_1|\pi_u$. Il suffit alors de montrer que P_1 annule u pour avoir l'autre divisibilité. Soit donc $z \in E$, que l'on décompose en $z = z_1 + \cdots + z_r$, avec $z_i \in k[u](x_i)$ pour tout i. Pour tout i, on a donc que $P_i(u)(z_i) = 0$. Mais pour tout i, P_i divise P_1 et donc pour tout i, $P_1(u)(z_i) = 0$. Finalement, $P_1(u)(z) = 0$, et donc $P_1 = \pi_u$.

Supposons qu'il existe un indice k_0 qui soit le plus petit entier tel que $P_{k_0} \neq Q_{k_0}$. Comme $P_1 = Q_1$, on a $k_0 \geq 2$.
Par hypothèse, on peut décomposer E de deux manières :

$$E = \bigoplus_{i=1}^{r} k[u](x_i) = \bigoplus_{j=1}^{s} k[u](y_j).$$

Appliquons $P_{k_0}(u)$ à ces égalités.

$$P_{k_0}(u)(E) = \bigoplus_{i=1}^{r} P_{k_0}(u)(k[u](x_i)) = \bigoplus_{j=1}^{s} P_{k_0}(u)(k[u](y_j)).$$

Par définition de k_0, on a $P_k = Q_k$ pour tout $k \leq k_0 - 1$. En particulier, pour tout $k \leq k_0 - 1$, on a $\dim(k[u](x_k)) = \dim(k[u](y_k))$.
D'autre part, comme pour tout $i \geq k_0$, P_i divise P_{k_0}, on a en fait $P_{k_0}(u)(k[u](x_i)) = 0$ pour tout $i \geq k_0$. D'où

$$\bigoplus_{i=1}^{k_0-1} P_{k_0}(u)(k[u](x_i)) = \bigoplus_{j=1}^{k_0-1} P_{k_0}(u)(k[u](y_j)) \oplus \bigoplus_{j=k_0}^{s} P_{k_0}(u)(k[u](y_j)).$$

En passant cette égalité aux dimensions, on obtient que

$$\dim\left(\bigoplus_{j=k_0}^{s} P_{k_0}(u)(k[u](y_j))\right) = 0.$$

Ainsi pour tout $j \in [\![k_0, s]\!]$, l'espace $P_{k_0}(u)(k[u](y_j))$ est l'espace nul, et en particulier $P_{k_0}(u)(y_j) = 0$. Par définition de $\pi_{u,y_j} = Q_j$, on a donc $P_j|Q_j$ pour tout $j \in [\![k_0, s]\!]$.
En opérant le même raisonnement avec Q_{k_0} au lieu de P_{k_0}, on trouve $Q_j|P_j$ pour tout $j \in [\![k_0, r]\!]$. Et ce sont des polynômes unitaires (définition de polynôme minimal), donc $Q_{k_0} = P_{k_0}$. Ceci est absurde au vu de la définition de k_0.

On vient ainsi de montrer que pour tout $k \in [\![1, r]\!]$, $P_k = Q_k$. Reste à vérifier que $r = s$. Ceci peut se faire en remarquant qu'on doit avoir $P_1 \cdots P_r = \chi_u = Q_1 \cdots Q_s$. En effet le produit $P_1 \cdots P_r$ annule u puisqu'il contient $P_1 = \pi_u$, il est de degré n grâce à l'hypothèse (ii) et il est unitaire car tous ses facteurs le sont.
Donc on a en fait $P_1 \cdots P_r = P_1 \cdots P_r Q_{r+1} \cdots Q_s$, ce qui implique bien sûr que $Q_{r+1} = \cdots = Q_s = 1$ (ils sont unitaires). Mais les polynômes Q_j ne sauraient être constants puisque ce sont des polynômes minimaux, et donc $r = s$. ■

3 Quelques conséquences

Ces corollaires sont bons à connaître, puisqu'ils peuvent faire l'objet de questions du jury.

Corollaire 3.1 Deux matrices sont semblables ssi elles ont les mêmes facteurs invariants.

Corollaire 3.2 Les facteurs invariants ne changent pas quand on se place sur une extension de corps. En particulier, le polynôme minimal est invariant par extension de corps.

Corollaire 3.3 Soient A et B deux matrices à coefficients dans k. Soit L une extension de k. Si A et B sont semblables sur L alors elles sont semblables sur k.

4 Lien avec la décomposition de Jordan

À partir de la réduction de Frobenius d'une matrice, on peut retrouver sa décomposition de Jordan. C'est un exercice qui peut être posé pendant la phase de questions, et qui peut aussi apparaître à l'écrit. On trouvera des explications détaillées dans le livre de Mansuy et Mneimné, *Algèbre linéaire - Réduction des endomorphismes*.

5 Lien avec la forme normale de Smith

La réduction de Frobenius est en fait un cas particulier de la mise sous forme normale de Smith dans l'anneau des matrices à coefficients polynomiaux. Il peut être intéressant de connaître les grandes lignes de cet algorithme de mise sous forme normale de Smith, surtout en option C. L'exposé de cette théorie peut se trouver dans *Matrices : theory and applications*, de Denis Serre.