# Invariants de similitudes et réduction de Frobenius

Marc SAGE

21 octobre 2005

## Table des matières

# 1 Endomorphismes cycliques

Soit $E$ un $K$-espace vectoriel de dimension $n$ non nulle. Considérons $f \in \mathcal{L}(E)$ un endomorphisme sur $E$.

On cherche des $x$ dans $E$ tels que $\left(x, f(x), ..., f^{n-1}(x)\right)$ soit une base de $E$, *i.e.* qui donnent une représentation "cyclique" de $f$.

## 1.1 Préliminaires – notations

Soit $f \in \mathcal{L}(E)$ et $x \in E$. On note respectivement :

- $\mu_f$ le polynôme minimal de $f$ ;
- $\chi_f$ le polynôme caractéristique de $f$ ;
- $\mathcal{L}_f$ l'ensemble des polynômes en $f$ :

$$\mathcal{L}_f = K[f] = \{P(f) \ ; P \in K[X]\} ;$$

- $E_x$ l'ensemble des polynômes en $f$ évalués en $x$ :

$$E_x = \mathcal{L}_f(x) = \{P(f)(x) \ ; P \in K[X]\} ;$$

- $\mathcal{I}_x$ l'idéal de $K[X]$ des polynômes annulant $f$ en $x$ :

$$\mathcal{I}_x = \{P \in K[X] \ ; P(f)(x) = 0\}.$$

$\mathcal{I}_x$ est principal en tant qu'idéal de l'anneau principal $K[X]$, n'est pas réduit à $(0)$ car $\mu_f(f)(x) = 0$, donc est engendré par un unique $\mu_x$ unitaire qui vérifie

$$P(f)(x) = 0 \iff \mu_x \mid P.$$

$\mu_x$ est appelé *polynôme minimal* de $x$ *relatif* à $f$.

**Remarques.**

- Si $\mu_f$ était constant, on aurait $0 = \mu_f(f) = 1(f) = \mathrm{Id}_E$ et $E = \{0\}$, ce qui exclu vu que l'on a supposé $\dim E \geq 1$. Il en résulte
$$\deg \mu_f \geq 1.$$
- Puisque $\mu_f(f)(x) = 0$, on a toujours
$$\forall x \in E, \ \mu_x \mid \mu_f.$$
- $\mu_x$ n'est jamais constant si $x$ est non nul : en effet, on a les équivalences

$$\begin{aligned} \deg \mu_x = 0 &\iff \mu_x = \lambda \text{ pour un certain } \lambda \neq 0 \\ &\iff \mu_x K[X] = K[X] \\ &\iff \mathcal{I}_x = K[X] \\ &\iff 1 \in \mathcal{I}_x \\ &\iff 0 = 1(f)(x) = \mathrm{Id}(x) = x. \end{aligned}$$

Ainsi,

$$\deg \mu_x \geq 1 \iff x \neq 0.$$

**Proposition (structure cyclique de $E_x$).**
*$E_x$ est un sous-espace vectoriel de dimension $\deg \mu_x$, stable par $f$, dont la base canonique est*

$$\left(x, f(x), ..., f^{\deg \mu_x - 1}(x)\right).$$

**Démonstration.**
Si $\deg \mu_x = 0$, alors $x = 0$ et $E_x$ est réduit à $\{0\}$ dont l'unique base est $\emptyset$. On suppose donc $\deg \mu_x \geq 1$.

Considérons l'application linéaire

$$\varphi : \left\{ \begin{array}{ccc} K[X] & \longrightarrow & E \\ P & \longmapsto & P(f)(x) \end{array} \right. ,$$

d'image $E_x$ et de noyau $\mathcal{I}_x$.

En factorisant canoniquement $\varphi$ selon ${}^{K[X]}\!/_{\operatorname{Ker}\varphi} \simeq \operatorname{Im}\varphi$, on obtient

$$\dim E_x = \dim\left({}^{K[X]}\!/_{\mathcal{I}_x}\right) = \dim\left({}^{K[X]}\!/_{(\mu_x)}\right) = \deg\mu_x.$$

On remarque par ailleurs que la famille $\left(x, f(x), ..., f^{\deg\mu_x - 1}(x)\right)$ est libre dans $E_x$ :

$$\sum_{i=0}^{\deg\mu_x - 1} \lambda_i f^i(x) = 0 \implies \sum_{i=0}^{\deg\mu_x - 1} \lambda_i X^i \in \mathcal{I}_x \implies \mu_x \mid \sum_{i=0}^{\deg\mu_x - 1} \lambda_i X^i \implies (\lambda_i) = 0$$

en prenant les degrés.

Pour obtenir la stabilité, il suffit de remarquer que $f^{\deg\mu_x}(x)$ reste dans $\operatorname{Vect}\left(x, f(x), ..., f^{\deg\mu_x - 1}(x)\right)$, ce qui s'obtient en écrivant $P(f)(x) = 0$.

**Définition.**

*Un endomorphisme $f \in \mathcal{L}(E)$ est dit* cyclique *s'il y a un $x$ dans $E$ tel que $\left(x, f(x), ..., f^{n-1}(x)\right)$ soit une base de $E$.*

*En d'autres termes, $f$ est cyclique ssi*

$$\exists x \in E,\ E_x = E,$$

*ou encore ssi*

$$\exists x \in E,\ E = \mathcal{L}_f(x).$$

**Proposition (structure cyclique de $\mathcal{L}_f$).**

*$\mathcal{L}_f$ est un sous-espace vectoriel de $\mathcal{L}(E)$ de dimension $\deg\mu_f$ dont la base canonique est*

$$\left(\mathrm{Id}, f, ..., f^{\deg\mu_f - 1}\right).$$

**Démonstration.**

Comme pour $E_x$, on considère l'application

$$\varphi : \left\{ \begin{array}{ccc} K[X] & \longrightarrow & \mathcal{L}(E) \\ P & \longmapsto & P(f) \end{array} \right. ,$$

d'image $\mathcal{L}_f$ et de noyau $\left(\mu_f\right)$, de sorte que

$$\dim\mathcal{L}_f = \dim\operatorname{Im}\varphi = \dim\ {}^{K[X]}\!/_{(\mu_f)} = \deg\mu_f.$$

On montre ensuite que la famille $\left(\mathrm{Id}, f, ..., f^{\deg\mu_f - 1}\right)$ est libre :

$$\sum_{i=0}^{\deg\mu_f - 1} \lambda_i f^i = 0 \implies \sum_{i=0}^{\deg\mu_f - 1} \lambda_i X^i \in \operatorname{Ker}\varphi \implies \mu_f \mid \sum_{i=0}^{\deg\mu_f - 1} \lambda_i X^i \implies (\lambda_i) = 0$$

en prenant les degrés.

**Remarque.** Si $F$ est un sous-espace vectoriel de $E$ stable par $f$ et $P$ un polynôme de $K[X]$, on a

$$P\left(f_{|F}\right) = P(f)_{|F}$$

(évaluer en un $x \in F$ quelconque), d'où pour $x \in F$

$$\mathcal{L}_{f_{|F}}(x) = \left\{P\left(f_{|F}\right)(x) \ ; \ P \in K[X]\right\} = \left\{P(f)_{|F}(x) \ ; \ P \in K[X]\right\} = \{P(f)(x) \ ; \ P \in K[X]\} = \mathcal{L}_f(x).$$

On en déduit la propriété

$$f_{|F} \text{ cyclique} \iff [\exists x \in F, \ \mathcal{L}_f(x) = F].$$

Étudions à présent le rapport entre la cyclicité d'un endomorphisme et son polynôme minimal.

## 1.2 Un résultat fondamental

La deuxième remarque des préliminaires affirme que $\mu_x \mid \mu_f$ pour tout vecteur $x$. L'égalité est en fait atteinte.

**Théorème.**
*Il existe un $x$ dans $E$ tel que*

$$\mu_x = \mu_f.$$

**Lemme 1.**
*On suppose que $\mu_f$ se factorise en*

$$\mu_f = P^\alpha A$$

*avec $P$ irréductible et $A$ premier avec $P$. Alors*

$$\exists x \in E, \ \mu_x = P^\alpha.$$

**Lemme 2.**
*Pour $x, y \in E$ on a l'implication*

$$\mu_x \wedge \mu_y = 1 \implies \mu_{x+y} = \mu_x \mu_y.$$

**Démonstration du théorème.**
On factorise $\mu_f$ en produit de facteurs irréductibles :

$$\mu_f = \prod_{i=1}^{r} P_i^{\alpha_i}.$$

Remarquer que le produit n'est pas vide car $\deg \mu_f \geq 1$.

Par le lemme 1, pour tout $i$ on peut trouver un $x_i$ dans $E$ tel que $\mu_{x_i} = P_i^{\alpha_i}$, et le lemme 2 nous affirme que

$$\mu_{x_1+\ldots+x_r} = \mu_{x_1} \ldots \mu_{x_r} = P_1^{\alpha_1} \ldots P_r^{\alpha_r} = \mu_f,$$

d'où l'élément recherché.

**Démonstration du lemme 1.**
Pour $x \in E$ donné, on dispose des implications

$$x \in \operatorname{Ker} P^\alpha(f) \implies P^\alpha(f)(x) = 0 \implies \mu_x \mid P^\alpha.$$

Si jamais $\mu_x \mid P^{\alpha-1}$ pour tout $x$ dans $\operatorname{Ker} P^\alpha(f)$, alors $P^{\alpha-1}A$ annule $f$ sur $\operatorname{Ker} P^\alpha(f)$ ; comme $P^{\alpha-1}A$ s'annule également sur $\operatorname{Ker} A(f)$ et que le lemme des noyaux nous donne $E = \operatorname{Ker} P^\alpha(f) \oplus \operatorname{Ker} A(f)$, on a finalement que $P^{\alpha-1}A$ annule $f$, d'où $\mu_f \mid P^{\alpha-1}A$, *absurde*.

Ainsi, il y a un $x$ tel que $\left\{ \begin{array}{c} \mu_x \mid P^\alpha \\ \mu_x \nmid P^{\alpha-1} \end{array} \right.$, *i.e.* $\mu_x = P^\alpha$ par irréductibilité de $P$, *CQFD.*

**Démonstration du lemme 2.**
On a $\mu_{x+y}(f)(y) = -\mu_{x+y}(f)(x)$, donc

$$0 = \mu_{x+y}\mu_y(f)(y) = \mu_y\mu_{x+y}(f)(y) = -\mu_y\mu_{x+y}(f)(x),$$

d'où $\mu_x \mid \mu_y\mu_{x+y}$ et $\mu_x \mid \mu_{x+y}$ en utilisant l'hypothèse de primalité. Par symétrie on obtient $\mu_y \mid \mu_{x+y}$, et on en déduit (toujours par primalité)

$$\mu_x\mu_y \mid \mu_{x+y}.$$

Par ailleurs, on a

$$\mu_x\mu_y(f)(x+y) = \mu_y\mu_x(f)(x) + \mu_x\mu_y(f)(y) = \mu_y(f)\underbrace{\mu_x(f)(x)}_{=0} + \mu_x(f)\underbrace{\mu_y(f)(y)}_{=0} = 0,$$

d'où la divisibilité réciproque

$$\mu_{x+y} \mid \mu_x\mu_y.$$

## 1.3 Cyclicité et polynôme minimal

**Proposition (cyclicité et polynôme minimal).**
*On dispose des équivalences*

$$f \text{ cyclique} \iff \deg\mu_f = n \iff \mu_f = \chi_f.$$

**Démonstration.**
Supposons$f$ cyclique et soit $x$ tel que $E_x = E$. On a alors

$$\deg\mu_x = \dim E_x = \dim E \geq \deg\mu_f \geq \deg\mu_x,$$

d'où $\deg\mu_f = n$, ce qui équivaut à $\mu_f = \chi_f$ par Cayley-Hamilton.

Réciproquement, si $\deg\mu_f = n$, alors par le théorème précédent il existe un $x \in E$ tel que $\mu_x = \mu_f = \chi_f$, d'où

$$\dim E_x = \deg\mu_x = \deg\mu_f = n$$

et $E_x = E$.

## 1.4 Cyclicité et matrices compagnons

Pour $P$ polynôme unitaire de degré $n$, disons

$$P = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0,$$

on notera $\mathcal{C}(P)$ la *matrice compagnon* de $P$, *i.e.*

$$\mathcal{C}(P) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix}.$$

On dit qu'une matrice $A \in \mathcal{M}_n(K)$ est *cyclique* si l'endomorphisme de $K^n$ qui lui est canoniquement associé est cyclique.

**Proposition (cyclicité et matrices compagnons).**
*Soit $f$ cyclique. Alors $f$ est semblable à la matrice compagnon de son polyôme minimal :*

$$f \text{ cyclique} \implies f \sim \mathcal{C}\left(\mu_f\right).$$

*Réciproquement, si $f$ est semblable à une matrice compagnon $\mathcal{C}(P)$, alors $f$ est cyclique de polynôme minimal $P$ :*

$$\left[\exists P \in K[X],\ f \sim \mathcal{C}(P)\right] \implies \left\{ \begin{array}{c} f \text{ cyclique} \\ \mu_f = P \end{array} \right. .$$

**Démonstration.**
Soit $f$ cyclique et $x \in E$ tel que $E_x = E$. On considère la base $\mathcal{B} = \left(x, f(x), ..., f^{n-1}(x)\right)$ de $E$ et on note

$$\mu_f = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0.$$

On écrit alors

$$\begin{array}{rcl} f^n(x) & = & f^n(x) - 0 \\ & = & f^n(x) - \mu_f(f)(x) \\ & = & f^n(x) - \left(f^n(x) + a_{n-1}f^{n-1}(x) + ... + a_1 f(x) + a_0 x\right) \\ & = & -a_{n-1}f^{n-1}(x) - ... - a_1 f(x) - a_0 x, \end{array}$$

d'où

$$\underset{\mathcal{B}}{\text{Mat}}\, f = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix} = \mathcal{C}\left(\mu_f\right).$$

Supposons réciproquement qu'il y a une base $\mathcal{B} = (e_1, ..., e_n)$ de $E$ et un polynôme $P$ de $K[X]$ tels que

$$\underset{\mathcal{B}}{\text{Mat}}\, f = \mathcal{C}(P) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix}.$$

On lit dans la matrice que $f(e_i) = e_{i+1}$ pour $i = 1, ..., n-1$, donc

$$\mathcal{B} = \left(e_1, f(e_1), f^2(e_1), ..., f^{n-1}(e_1)\right),$$

d'où la cyclicité de $f$.

**Remarque.** La proposition précédente permet d'obtenir sans effort le polynôme minimal d'une matrice compagnon. En effet, pour $P \in K[X]$, la matrice $\mathcal{C}(P)$ est clairement cyclique dans la base canonique de $K^n$, d'où

$$\mu_{\mathcal{C}(P)} = \chi_{\mathcal{C}(P)} = P.$$

Nous allons à présent montrer que l'on peut toujours casser l'espace ambiant $E$ en sous-espaces stables sur lesquels $f$ est cyclique (à l'exemple de $E_x$).

# 2 Invariants de similitude et réduction de Frobenius

## 2.1 Suite des invariants de similitude

**Théorème (invariants de similitudes).**
*Soit $f \in \mathcal{L}(E)$. Il existe $F_1, ..., F_r$ des sous-espaces vectoriels de $E$ non réduits à $\{0\}$ tels que*
*(i)* $E = F_1 \oplus ... \oplus F_r$ ;
*(ii)* $F_i$ *est stable par* $f$ *et* $f_{|F_i}$ *est cyclique ;*
*(iii)* *en posant* $\mu_i = \mu_{f_{|F_i}}$, *on a la suite de divisibilités*

$$\mu_r \mid \mu_{r-1} \mid ... \mid \mu_2 \mid \mu_1 = \mu_f.$$

*Par ailleurs, la suite* $(\mu_1, ..., \mu_r)$ *ne dépend que de* $f$ *et non des* $F_i$ *; on l'appelle la* suite des invariants de similitude *de* $f$.

**Démonstration.**

*Existence.*
Par récurrence sur $n$. Notons $\nu = \deg \mu_f \in \mathbb{N}^*$.
Soit $x \in E$ tel que $\mu_x = \mu_f$ et notons $e_i = f^{i-1}(x)$ pour $i = 1, ..., \nu$. On sait que

$$E_x = Ke_1 \oplus Ke_2 \oplus ... \oplus Ke_\nu$$

est stable par $f$ en vertu de l'identité $\mu_f(f)(x) = 0$ (laquelle montre que $f^\nu(x)$ reste dans $\mathrm{Vect}\left(x, f(x), ..., f^{\nu-1}(x)\right)$). Cette dernière égalité nous permet en outre d'écrire $\mathrm{Mat}_{(e_1,...,e_\nu)} f_{|E_x} = \mathcal{C}\left(\mu_f\right)$, donc $f_{|E_x}$ est cyclique et $\mu_{f_{|E_x}} = \mu_f$. Enfin, $\dim E_x = \nu \geq 1$, donc $E_x$ n'est pas réduit à $\{0\}$. Tout cela fait de $E_x$ un bon candidat pour $F_1$. Il faut maintenant trouver un "gentil" supplémentaire de $E_x$ sur lequel on pourra récurrer.

Complétons $(e_1, ..., e_\nu)$ en une base quelconque de $E$, de sorte que l'on puisse parler des $e_i^*$ dans cette base. On pose successivement

$$\begin{array}{rcl} F & = & Ke_1 \oplus Ke_2 \oplus ... \oplus Ke_\nu, \\ \Gamma & = & \left\{e_\nu^* \circ f^i ;\ i \in \mathbb{N}\right\} \subset E^*, \\ G & = & \Gamma^\circ \quad \text{(orthogonal dual).} \end{array}$$

On a déjà dit que $F = E_x$ était stable par $f$, et il est en outre clair que $G$ est stable par $f$ :

$$x \in \Gamma^\circ \implies \forall i \in \mathbb{N},\ e_\nu^* \circ f^i(x) = 0 \implies \forall i \in \mathbb{N},\ e_\nu^* \circ f^i(f(x)) = 0 \implies f(x) \in \Gamma^\circ.$$

Montrons maintenant que $F \oplus G = E$.

Soit $y \in F \cap G$ non nul. Puisque $y \in F$, $y$ s'écrit $\sum_{i=1}^p \lambda_i e_i$ où $\left\{ \begin{array}{c} 1 \leq p \leq \nu \\ \lambda_p \neq 0 \end{array} \right.$ ($p$ est le plus grand indice $i$ tel que $\lambda_i \neq 0$). Comme de plus $y \in G$, on a

$$\begin{array}{rcl} 0 & = & e_\nu^* \circ f^{\nu-p}(y) = e_\nu^* \circ f^{\nu-p}\left(\sum_{i=1}^p \lambda_i e_i\right) = e_\nu^*\left(\sum_{i=1}^p \lambda_i f^{\nu-p}(e_i)\right) \\ & = & e_\nu^*\left(\sum_{i=1}^p \lambda_i e_{\nu-p+i}\right) = \sum_{i=1}^p \lambda_i e_\nu^*(e_{\nu-p+i}) = \sum_{i=1}^p \lambda_i \delta_\nu^{\nu-p+i} = \lambda_p, \text{ absurde.} \end{array}$$

On veut maintenant $\dim F + \dim G = n$, ce qui équivaut sucessivement à

$$\dim E_x = n - \dim G \iff \deg \mu_x = n - \dim \Gamma^\circ \iff \dim \mathcal{L}_f = \dim \mathrm{Vect}\,\Gamma.$$

On considère pour cela l'application linéaire

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}_f & \longrightarrow & \mathrm{Vect}\,\Gamma \\ P(f) & \longmapsto & e_\nu^* \circ P(f) \end{array} \right.$$

clairement surjective, et on montre son injectivité. Soit $u \in \operatorname{Ker}\varphi$ non nul : on peut toujours écrire $u = \sum_{i=0}^{p} \lambda_i f^i$ où $\left\{ \begin{array}{c} 0 \leq p < \nu \\ \lambda_p \neq 0 \end{array} \right.$, d'où

$$\begin{aligned} 0 &= e_\nu^* \circ u\left(f^{\nu-p-1}(x)\right) = e_\nu^* \circ \left(\sum_{i=0}^{p} \lambda_i f^{i+\nu-p-1}(x)\right) = e_\nu^* \left(\sum_{i=0}^{p} \lambda_i e_{i+\nu-p}\right) \\ &= \sum_{i=0}^{p} \lambda_i e_\nu^*\left(e_{i+\nu-p}\right) = \sum_{i=0}^{p} \lambda_i \delta_\nu^{i+\nu-p} = \lambda_p, \textit{ absurde.} \end{aligned}$$

Ainsi $\varphi$ est un isomorphisme, d'où l'égalité des dimensions

$$\dim \mathcal{L}_f = \dim \operatorname{Vect}\Gamma.$$

Dans le cas où $\dim G = 0$, on a terminé. Sinon, puisque $\mu_{f_{|F}} = \mu_{f_{|E_x}} = \mu_f$, $\mu_{f_{|F}}$ annule $f$, donc annule $f_{|G}$, d'où $\mu_{f_{|G}} \mid \mu_{f_{|F}} = \mu_f$. Il suffit alors de récurrer en se plaçant sur le sous-espace $G$ (qui est bien de dimension $\geq 1$).

*Unicité.*

Supposons que $\left\{ \begin{array}{c} F_1, ..., F_r \\ G_1, ..., G_s \end{array} \right.$ vérifient les conditions du théorème. On peut toujours supposer $r \leq s$ par symétrie. Notons $\left\{ \begin{array}{c} P_i = \mu_{f_{|F_i}} \\ Q_j = \mu_{f_{|G_j}} \end{array} \right.$. On veut

$$(P_1, ..., P_r) = (Q_1, ..., Q_s).$$

Si ce n'est pas le cas, on peut considérer $k_0$ le plus petit indice $k \leq r$ tel que $P_k \neq Q_k$. Un tel $k_0$ existe, sinon on aurait $(P_1, ...P_r) = (Q_1, ..., Q_r)$, d'où

$$\sum_{i=1}^{r} \deg P_i = \sum_{i=1}^{r} \dim F_i = n = \sum_{j=1}^{s} \dim G_j = \sum_{j=1}^{s} \deg Q_j = \sum_{j=1}^{r} \deg P_j + \sum_{j=r+1}^{s} \deg Q_j$$

et

$$\sum_{j=r+1}^{s} \deg Q_j = 0,$$

ce qui force $s \leq r$ puis $s = r$, d'où

$$(P_1, ...P_r) = (Q_1, ..., Q_r) = (Q_1, ..., Q_s), \textit{ exclu.}$$

Ensuite, en notant $\pi = P_{k_0}(f)$, puisque que tous les $F_i$ sont stables par $f$, donc par tout polynôme en $F$, *a fortiori* par $\pi$, on peut écrire

$$\begin{aligned} \pi(E) &= \pi(F_1 \oplus ... \oplus F_r,) = \pi(F_1) \oplus ... \oplus \pi(F_r) \\ &= \pi(F_1) \oplus ... \oplus \pi(F_{k_0-1}) \oplus [\pi(F_{k_0}) \oplus ... \oplus \pi(F_r)]; \end{aligned}$$

on a de même

$$\pi(E) = \pi(G_1) \oplus ... \oplus \pi(G_{k_0-1}) \oplus [\pi(G_{k_0}) \oplus ... \oplus \pi(G_s)].$$

On va montrer qu'en fait $\left\{ \begin{array}{c} \pi(F_{k_0}) \oplus ... \oplus \pi(F_r) = \{0\} \\ \pi(G_{k_0}) \oplus ... \oplus \pi(G_s) = \{0\} \end{array} \right.$.

Soit $i$ un indice tel que $k_0 \leq i \leq r$.

Par hypothèse, $P_r \mid ... \mid P_{k_0+1} \mid P_{k_0}$, donc $P_i \mid P_{k_0}$, d'où successivement

$$\mu_{f_{|F_i}} \mid P_{k_0} \implies P_{k_0}\left(f_{|F_i}\right) = 0 \implies P_{k_0}(f)_{|F_i} = 0 \implies \pi_{|F_i} = 0 \implies \dim \pi(F_i) = 0.$$

Soit maintenant $i$ un indice tel que $1 \leq i < k_0$.

Toujours par hypothèse, $f_{|F_i}$ est cyclique, donc est semblable à $\mathcal{C}\left(\mu_{f_{|F_i}}\right) = \mathcal{C}(P_i)$, et de même $f_{|G_i} \sim \mathcal{C}(Q_i) = \mathcal{C}(P_i)$ car $(P_1, ..., P_{k_0-1}) = (Q_1, ..., Q_{k_0-1})$. On en déduit

$$f_{|F_i} \sim f_{|G_i} \implies P_{k_0}\left(f_{|F_i}\right) \sim P_{k_0}\left(f_{|G_i}\right) \implies \pi_{|F_i} \sim \pi_{|G_i} \implies \operatorname{rg}\pi_{|F_i} = \operatorname{rg}\pi_{|G_i} \implies \dim \pi(F_i) = \dim \pi(G_i).$$

En reprenant les deux "cassages" de $\pi(E)$ ci-dessus

$$\pi(E) = \left| \begin{array}{l} \underbrace{\pi(F_1) \oplus ... \oplus \pi(F_{k_0-1})}_{\text{même dimension}} \oplus \underbrace{[\pi(F_{k_0}) \oplus ... \oplus \pi(F_r)]}_{=0} \\ \underbrace{\pi(G_1) \oplus ... \oplus \pi(G_{k_0-1})}_{} \oplus [\pi(G_{k_0}) \oplus ... \oplus \pi(G_s)] \end{array} \right. ,$$

on obtient

$$\begin{aligned} \dim[\pi(G_{k_0}) \oplus ... \oplus \pi(G_s)] = 0 \quad &\Longrightarrow \quad \dim \pi(G_{k_0}) = 0 \implies \pi_{|G_{k_0}} = 0 \\ &\Longrightarrow \quad P_{k_0}\left(f_{|G_{k_0}}\right) = 0 \implies \mu_{f_{|G_{k_0}}} \mid P_{k_0} \implies Q_{k_0} \mid P_{k_0}. \end{aligned}$$

Un argument symétrique nous donnerait l'autre sens, d'où l'égalité $P_{k_0} = Q_{k_0}$ qui contredirait la définition de $k_0$.

## 2.2 Réduction de Frobenius

**Théorème (réduction de Frobenius).**
*Si $\mu_1, ..., \mu_r$ est la suite des invariants de similitude de $f$, il existe une base $\mathcal{B}$ de $E$ où*

$$\underset{\mathcal{B}}{\text{Mat}}\, f = \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}.$$

*De plus :*

$$\begin{cases} \mu_f = \mu_1 \\ \chi_f = \mu_1 ... \mu_r \end{cases}.$$

**Démonstration.**
La réduction découle directement du théorème précédent et du fait qu'un endomorphisme cyclique est semblable à la matrice compagnon de son polynôme minimal.
Pour obtenir le polynôme caractéristique, il suffit d'écrire

$$\chi_f = \chi \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix} = \chi_{\mathcal{C}(\mu_1)} \cdots \chi_{\mathcal{C}(\mu_r)} = \mu_1 ... \mu_r \text{ par construction de la matrice compagnon.}$$

**Corollaire (caractérisation des classes de similitudes).**
*Deux endomorphismes sont semblables ssi ils ont la même suite d'invariants de similitude.*

**Lemme.**
*Soit $f \in \mathcal{L}(E)$, $\varphi \in \mathcal{GL}(E)$ et $g = \varphi f \varphi^{-1}$. On se donne $F$ un sous-espace vectoriel de $E$ stable par $f$. Alors :*
*(i)* $\varphi(F)$ *est stable par* $g$ *;*
*(ii)* $f_{|F}$ *cyclique* $\implies$ $g_{|\varphi(F)}$ *cyclique ;*
*(iii)* $\mu_{g_{|\varphi(F)}} = \mu_{f_{|F}}$.

**Démonstration du lemme.**
*(i)* Supposons $f(F) \subset F$. Alors

$$g(\varphi(F)) = g\varphi(F) = \varphi f \varphi^{-1} \varphi(F) = \varphi \underbrace{f(F)}_{\subset F} \subset \varphi(F),$$

donc $\varphi(F)$ est stable par $g$.

(*ii*) Supposons $f_{|F}$ cyclique. Par la dernière remarque des préliminaires, il y a un $x_0 \in F$ (mieux que $x_0 \in E$) tel que

$$F = \mathcal{L}_f(x_0).$$

En remarquant que pour $P \in K[X]$ on a

$$\begin{aligned} \varphi(P(f(x_0))) &= \varphi \circ P(f)(x_0) = \varphi \circ P\left(\varphi^{-1} g \varphi\right)(x_0) = \left[\varphi \circ \varphi^{-1} P(g)\varphi\right](x_0) \\ &= [P(g)\varphi](x_0) = P(g)(\varphi(x_0)), \end{aligned}$$

on dispose des équivalences

$$\begin{aligned} y \in \varphi(F) &\iff \exists x \in F,\ y = \varphi(x) \\ &\iff \exists x \in \mathcal{L}_f(x),\ y = \varphi(x) \\ &\iff \exists P \in K[X],\ y = \varphi(P(f(x_0))) \\ &\iff \exists P \in K[X],\ y = P(g)[\varphi(x_0)] \\ &\iff y \in \mathcal{L}_g(\varphi(x_0)), \end{aligned}$$

d'où $\varphi(F) = \mathcal{L}_g(\varphi(x_0))$, et $g_{|\varphi(F)}$ cyclique.

(*iii*) Soit $P \in K[X]$. En écrivant

$$P\left(g_{|\varphi(F)}\right) = P(g)_{|\varphi(F)} = P\left(\varphi f \varphi^{-1}\right)_{|\varphi(F)} = \varphi P(f) \varphi^{-1}_{|\varphi(F)},$$

on a par équivalences

$$\begin{aligned} P\left(g_{|\varphi(F)}\right) = 0 &\iff \forall y \in \varphi(F),\ P\left(g_{|\varphi(F)}\right)(y) = 0 \\ &\iff \forall x \in F,\ \left[\varphi P(f) \varphi^{-1}_{|\varphi(F)}\right](\varphi(x)) = 0 \\ &\iff \forall x \in F,\ \varphi P(f)(x) = 0 \\ &\iff \varphi \circ P\left(f_{|F}\right) = 0 \\ &\iff P\left(f_{|F}\right) = 0 \text{ car } \varphi \text{ est inversible,} \end{aligned}$$

de sorte que les polynômes annulateurs de $g_{|\varphi(F)}$ sont les mêmes que ceux de $f_{|F}$ ; par conséquent, les générateurs unitaires de ces idéaux coïncident, *i.e.* $\mu_{g_{|\varphi(F)}} = \mu_{f_{|F}}$, *CQFD.*

**Démonstration du corollaire.**

Soient $f$ et $g$ deux endomorphismes semblables, mettons $g = \varphi f \varphi^{-1}$ où $\varphi$ isomorphisme. Considérons des $F_1, ..., F_r$ associés à $f$ comme dans le théorème. En posant $G_i = \varphi(F_i)$, on a

$$E = \varphi(E) = \varphi(F_1 \oplus ... \oplus F_r) = \varphi(F_1) \oplus ... \oplus \varphi(F_r) = G_1 \oplus ... \oplus G_r.$$

Par ailleurs, le lemme nous dit que les $G_i$ sont stables par $g$, que les $g_{|G_i}$ sont cycliques et que $\mu_{g_{|G_i}} = \mu_{f_{|F_i}}$. Comme d'autre part on a $\mu_g = \mu_f$ (deux endorphismes semblables ont même polynôme minimal), du dernier point on déduit

$$\mu_{g_{|G_r}} \mid \mu_{g_{|G_{r-1}}} \mid ... \mid \mu_{g_{|G_2}} \mid \mu_{g_{|G_1}} = \mu_g.$$

Par l'unicité du théorème, les $\mu_{g_{|G_i}} = \mu_{f_{|F_i}}$ sont les invariants de similitudes de $g$, d'où le résultat.

Le sens réciproque est trivial en appliquant la réduction de Frobenius.

# 3 Applications

## 3.1 Commutant et cyclicité

On note $\operatorname{Comm} f$ le commutant d'un endomorphisme $f$ :

$$\operatorname{Comm} f = \{u \in \mathcal{L}(E);\ uf = fu\}.$$

**Proposition.**
*On a l'équivalence*

$$f \text{ cyclique} \iff \operatorname{Comm} f = K[f].$$

**Démonstration.**
$\boxed{\Longrightarrow}$ Soit $u \in \operatorname{Comm}(f)$. $f$ est cyclique, donc $E = \mathcal{L}_f(x)$ pour un $x$ bien choisi. Ainsi, $u(x)$ s'écrit $P(f)(x)$. Montrons qu'en fait $u = P(f)$ pour le $P$ considéré.

Soit $y$ quelconque dans $E$, que l'on écrit $Q(f)(x)$. Puisque $\operatorname{Comm} f \subset \operatorname{Comm} Q(f)$, $u$ commute avec $Q(f)$, d'où

$$u(y) = u \circ Q(f)(x) = Q(f) \circ u(x) = Q(f) \circ P(f)(x) = P(f) \circ Q(f)(x) = P(f)(y),$$

d'où $u = P(f) \in K[X]$ et $\operatorname{Comm}(f) \subset K[X]$. L'inclusion réciproque est évidente.

$\boxed{\Longleftarrow}$ D'après le théorème des invariants de similitude, on peut écrire

$$E = F_1 \oplus F_2 \oplus ... \oplus F_r$$

avec les $F_i$ qui vérifient les bonnes propriétés. L'idée est de montrer que $r = 1$, de sorte que $f = f_{|F_1}$ est cyclique.

Soit $\pi$ la projection sur $F_2 \oplus ... \oplus F_r$ parallèlement à $F_1$. Puisque $F_1$ et $F_2 \oplus ... \oplus F_r$ sont stables par $f$, $\pi$ commute avec $f$, *i.e.* $\pi \in \operatorname{Comm} f = K[X]$, et donc s'écrit

$$\pi = P(f)$$

pour un certain polynôme $P$. On a alors les implications

$$\begin{aligned}
F_1 = \operatorname{Ker}\pi &\implies \pi_{|F_1} = 0 \implies P\left(f_{|F_1}\right) = 0 \implies \mu_{f_{|F_1}} \mid P \\
&\implies \forall i \in \{1,...,r\},\ \mu_{f_{|F_i}} \mid P \ (\text{car } \mu_{f_{|F_i}} \mid \mu_{f_{|F_1}}) \\
&\implies \forall i \in \{1,...,r\},\ P\left(f_{|F_i}\right) = 0 \\
&\implies \forall i \in \{1,...,r\},\ \pi_{|F_i} = 0 \\
&\implies \pi = 0 \text{ car } E = F_1 \oplus F_2 \oplus ... \oplus F_r \\
&\implies \operatorname{Im}\pi = \{0\} \\
&\implies F_2 \oplus ... \oplus F_r = \{0\} \\
&\implies r = 1 \text{ car } F_i \neq \{0\} \text{ pour tout } i \\
&\implies f = f_{|E} = f_{|F_1} \text{ est cyclique, comme souhaité.}
\end{aligned}$$

## 3.2 Réduction de Jordan

**Théorème.**
*Soit $K$ algébriquement clos et $E$ un $K$-espace vectoriel de dimension non nulle.*

*Soit $f$ un endomorphisme sur $E$ dont on note $\lambda_1, ..., \lambda_p$ les valeurs propres ($\operatorname{Sp} f \neq \emptyset$ par l'hypothèse de clôture algébrique).*

*Alors $f$ est semblable à une matrice de la forme*

$$f \sim \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix}$$

*où chaque $J_k$ (appelé* bloc de Jordan*) est de la forme*

$$\begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

*avec $\lambda$ valeur propre de $f$ (noter qu'une même valeur propre $\lambda$ peut apparaître dans deux blocs de Jordan $J_k$ différents).*

*Un autre forme possible (équivalente en regroupant les valeurs propres identiques) est la suivante :*

$$f \sim \begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & \varepsilon_1^{(1)} & & \\ & \ddots & \ddots & \\ & & \ddots & \varepsilon_{\alpha_1}^{(1)} \\ & & & \lambda_1 \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} \lambda_p & \varepsilon_1^{(p)} & & \\ & \ddots & \ddots & \\ & & \ddots & \varepsilon_{\alpha_p}^{(p)} \\ & & & \lambda_p \end{matrix}} \end{pmatrix}$$

*où tous les $\varepsilon_j^{(i)}$ sont à valeurs dans $\{0,1\}$.*

**Démonstration.**

On regarde tout d'abord le cas d'un endomorphisme $f$ nilpotent.

Un tel $f$ a nécessairement son polynôme minimal de la forme $\mu_f = X^p$ où $p$ est le degré de nilpotence de $f$, donc les matrices compagnons des invariants de similitude de $f$ sont du type $\begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}$. Or, si

$$\underset{(e_1,\ldots,e_k)}{\mathrm{Mat}}\ u = \begin{pmatrix} 0 & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix},$$

en inversant l'ordre des vecteurs, on a

$$\underset{(e_k,\ldots,e_1)}{\mathrm{Mat}}\ u = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix},$$

de sorte que $f$ est semblable à une matrice du type

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{matrix}} \end{pmatrix}.$$

On revient à présent au cas général, et on considère les espaces caractéristiques

$$N_i = \mathrm{Ker}\,(f - \lambda_i\,\mathrm{Id})^{\alpha_i}$$

où $\alpha_i$ est la multiplicité de la valeur propre $\lambda_i$ dans le polynôme minimal de $f$

$$\mu_f = \prod_{i=1}^{p} (X - \lambda_i)^{\alpha_i}$$

que l'on a scindé en utilisant l'hypothèse de clôture algébrique. Observer que les $N_i$ sont stables : $f$ commutant avec tout polynôme en $f$, $f$ commute avec $(f - \lambda_i \operatorname{Id})^{\alpha_i}$, donc le noyau $N_i$ de ce dernier est stable.

On considère l'endomorphisme $f_{|N_i} - \lambda_i \operatorname{Id}_{N_i}$, qui est clairement nilpotent, et on utilise ce qui précède pour obtenir une base $\mathcal{B}_i$ de $N_i$ dans laquelle

$$\operatorname*{Mat}_{\mathcal{B}_i}\left(f_{|N_i} - \lambda_i \operatorname{Id}_{N_i}\right) = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{matrix}} \end{pmatrix},$$

d'où

$$\operatorname*{Mat}_{\mathcal{B}_i} f_{|N_i} = \begin{pmatrix} \boxed{\begin{matrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{matrix}} \end{pmatrix}.$$

Il suffit alors de recoller les bases $\mathcal{B}_i$ pour obtenir la forme voulue, en remarquant que

$$\begin{aligned} E &= \operatorname{Ker} \mu_f(f) \\ &= \operatorname{Ker}\left[(f - \lambda_1 \operatorname{Id})^{\alpha_1} ... (f - \lambda_p \operatorname{Id})^{\alpha_p}\right] \\ &= \operatorname{Ker}(f - \lambda_1 \operatorname{Id})^{\alpha_1} \oplus ... \oplus \operatorname{Ker}(f - \lambda_p \operatorname{Id})^{\alpha_p} \quad \text{(lemme des noyaux)} \\ &= N_1 \oplus ... \oplus N_p. \end{aligned}$$

## 3.3 Matrices semblables et extensions de corps

On appelle *suite des invariants de similitude* d'une matrice $A \in \mathcal{M}_n(K)$ la suite des invariants de similitude de l'endomophisme de $K^n$ canoniquement associé à $A$.

**Proposition (conservation des invariants de similitude par extension de corps).**
*Soit $A \in \mathcal{M}_n(K)$ et $K \hookrightarrow L$ une extension de corps – i.e. un morphisme de corps (qui est nécessairement injectif), par exemple l'injection canonique de $\mathbb{R}$ dans $\mathbb{C}$.*

*Alors la suite des invariants de similitude de $A$ vue dans $\mathcal{M}_n(L)$ est la même que celle de $A$, à un plongement $K[X] \hookrightarrow L[X]$ près.*

**Démonstration.**

On note $\widetilde{A}$ la matrice $A$ vue dans $M_n(L)$ et

$$\begin{cases} f \text{ l'endomorphisme de } \mathcal{L}(K^n) \text{ associé à } A \\ \widetilde{f} \text{ l'endomorphisme de } \mathcal{L}(L^n) \text{ associé à } \widetilde{A} \end{cases}.$$

Par Frobenius appliqué à $f$, il existe une base $\mathcal{B}$ de $K^n$ dans laquelle

$$\underset{\mathcal{B}}{\text{Mat}}\, f = \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}$$

où $\mu_1, ..., \mu_r$ sont les invariants de similitude de $f$ (donc de $A$). Notons $\mathcal{B}_c$ la base canonique de $K^n$, de sorte que

$$A = \underset{\mathcal{B}_c}{\text{Mat}}\, f = P \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix} P^{-1}$$

où $P$ est la matrice de passage de $\mathcal{B}_c$ à $\mathcal{B}$. En plongeant cela dans $\mathcal{M}_n(L)$, on obtient

$$\widetilde{A} = P \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix} P^{-1},$$

d'où l'existence d'une base $\mathcal{B}'$ de $L^n$ (donnée $P$ en tant que matrice de passage) où

$$\underset{\mathcal{B}'}{\text{Mat}}\, \widetilde{f} = \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}.$$

En regroupant les éléments de $\mathcal{B}'$ selon les blocs ci-dessus, on définit des sous-espace vectoriels $F_1, ..., F_r$ de $L^n$ stables par $\widetilde{f}$ tels que $F_1 \oplus ... \oplus F_r = L^n$ et sur chacun desquels la restriction de $\widetilde{f}$ est cyclique de polynôme minimal $\mu_{\widetilde{f}_{|F_i}} = \mu_{\mathcal{C}(\mu_i)} = \mu_i$, de sorte que les $\mu_{\widetilde{f}_{|F_i}}$ vérifient les mêmes relations de divisibilités que les $\mu_i$. On en déduit que les $\mu_{\widetilde{f}_{|F_i}} = \mu_i$ (plongés dans $L[X]$) sont les invariants de similitudes de $\widetilde{f}$.

**Corollaire.**
*Soient $A$ et $B$ deux matrices dans $\mathcal{M}_n(K)$ et $K \hookrightarrow L$ une extension de corps.*
*On suppose que $A$ et $B$ sont semblables dans $\mathcal{M}_n(L)$. Alors elles sont semblables dans $\mathcal{M}_n(K)$ :*

$$\begin{cases} A, B \in \mathcal{M}_n(K) \\ A \underset{\mathcal{M}_n(L)}{\sim} B \end{cases} \implies A \underset{\mathcal{M}_n(K)}{\sim} B.$$

**Démonstration.**
Puisque $A \underset{\mathcal{M}_n(L)}{\sim} B$, $A$ et $B$ ont mêmes invariants de similitude dans $L[X]$ ; or ces invariants sont déjà dans $K[X]$ puisque $A$ et $B$ sont à coefficients dans $K$, d'où $A \underset{\mathcal{M}_n(K)}{\sim} B$.

**Remarque.** Ce résultat est un exercice archi-classique dans le cas de l'extension $\mathbb{R} \hookrightarrow \mathbb{C}$ qui se généralise aisément à une extension d'un corps infini (cf. feuille sur les déterminants). Pour le cas fini, il semble nécessaire de faire appel à un argument de toute autre nature (ici les invariants de similitude)

## 3.4 Rang et degré du polynôme minimal

*Montrer qu'en dimension finie tout endomorphisme $u$ de rang $r$ possède un polynôme annulateur $P$ de degré au plus $r+1$.*

**Solution proposée.**
Soit $\begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}$ la réduite de Frobenius de $A$ où $\mu_r \mid ... \mid \mu_1 = \mu_A$. Posons $\mu_0 = 1$ et soit $s$ le plus petit indice tel que $X$ ne divise pas $\mu_s$ ($s$ existe vue la définitino de $\mu_0$), de sorte que $X$ divise les $r-s$ polynômes $\mu_{s+1}, \mu_{s+2}, ..., \mu_r$.

Il est aisé de calculer le rang d'une matrice compagnon :

$$\operatorname{rg}\mathcal{C}(P) = \begin{pmatrix} 0 & & & -P(0) \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & ? \\ & & 1 & ? \end{pmatrix} = \begin{cases} \deg P - 1 \text{ si } P(0) = 0 \\ \deg P \text{ sinon} \end{cases} = \deg P - \{X \mid P\ ?\}.$$

où $\{p\ ?\}$ dénote la valeur logique (0 ou 1) de la proposition $p$.

En notant $n_i$ les degrés des $\mu_i$, et en remarquant que $\deg \mu_A = n_r$, il vient

$$\begin{aligned} \operatorname{rg} A &= \sum_{i=1}^{r} (n_i - \{X \mid \mu_i\ ?\}) = \left(\sum_{i=1}^{r} n_i\right) - (r-s) \geq n_r + (r-1) - (r-s) = \deg \mu_A + (s-1) \\ &\geq \deg \mu_A - 1, \ \textit{CQFD.} \end{aligned}$$

**Remarque.** Cette inégalité est optimale, vu que tout nilpotent $u$ cyclique vérifie $\mu_u = \chi_u = X^n$ et $\operatorname{rg} u = n-1$ : regarder $u$ comme la matrice $\begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$.

## 3.5 Une formule explicite pour le polynôme caractéristique

Pour une matrice $A \in M_n(K)$ et $I$ une partie de $\{1, ..., n\}$, on notera $A_I$ la matrice extraite $(a_{i,j})_{i,j\in I}$.

*Montrer la formule suivante :*

$$\det(A + tI_n) = \sum_{I \subset \{1,...,n\}} (\det A_I)\, t^{n-|I|}.$$

*Commenter le rapport avec le polynôme caractéristique.*

**Démonstration.**
Nous allons partir de la quantité de droite, que l'on notera $D(A)$ ("D" comme "**d**éterminant"), et montrer qu'elle vaut le membre de gauche. L'idée est de montrer le résulat sur les matrices cycliques, de les recoller, puis d'utiliser Frobenius pour conclure.

Trois étapes se distinguent ainsi tout naturellement : d'une part vérifier l'égalité voulue pour les matrices cycliques, d'autre part vérifier que $D\begin{pmatrix} A & \\ & B \end{pmatrix} = D(A)\,D(B)$, puis montrer que $D$ est invariante par conjugaison. Frobenius permettra alors d'écrire, si $A = P\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{pmatrix} P^{-1}$ où chaque $C_i$ est cyclique :

$$\begin{aligned} D(A) &= D\left(P\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{pmatrix} P^{-1}\right) = D\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{pmatrix} = D(C_1)\ldots D(C_r) \\ &= \det(C_1 + t\,\mathrm{Id})\ldots\det(C_r + t\,\mathrm{Id}) = \det\begin{pmatrix} C_1 + t\,\mathrm{Id} & & \\ & \ddots & \\ & & C_r + t\,\mathrm{Id} \end{pmatrix} \\ &= \det\left(\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{pmatrix} + t\,\mathrm{Id}\right) = \det\left(P\left[\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{pmatrix} + t\,\mathrm{Id}\right]P^{-1}\right) \\ &= \det(A + t\,\mathrm{Id}),\ \textit{CQFD.} \end{aligned}$$

Première étape : vérifier la formule pour $A = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix}$ cyclique. On veut

$$\begin{aligned} D(A) &\overset{?}{=} \det(A + tI_n) \\ \sum_{k=0}^{n}\left(\sum_{|I|=k}\det A_I\right)t^{n-k} \overset{?}{=} (-1)^n\chi_A(-t) &= t^n - a_{n-1}t^{n-1} + \ldots + (-1)^n a_0 \\ \forall k &= 0,\ldots,n,\ \sum_{|I|=k}\det A_I \overset{?}{=} (-1)^k a_{n-k}. \end{aligned}$$

Montrons que presque tous les $\det A_I$ sont nuls. Déjà, si $n \notin I$, la matrice extraite est triangulaire inférieure de diagonale nulle, d'où $\det A_I = 0$. Ensuite, en ordonnant les éléments de $I$ selon $i_1 < \ldots < i_k = n$, $A_I$ aura pour tête quelque chose du style

$$\begin{pmatrix} 0 & & & \alpha_1 \\ \varepsilon_1 & \ddots & & \vdots \\ & \ddots & 0 & \alpha_{k-1} \\ & & \varepsilon_{k-1} & \alpha_k \end{pmatrix} \text{ où } \varepsilon_p \in \{0,1\},$$

d'où son déterminant en développant selon la première ligne : en particulier, $\det A_I$ sera nul si l'un des $\varepsilon_p$ vaut 0. Or, on obtient $\varepsilon_p$ en prenant le coefficient en bas à gauche de la matrice $A_{\{i_p,i_{p+1}\}}$, lequel vaut 1 ssi $i_{p+1} = i_p + 1$. Pour que tous les $\varepsilon_i$ soient non nuls, il faut donc que tous les $i_p$ soient consécutifs, ce qui ne laisse plus qu'un choix pour $A_I$ : le bloc tout en bas à droite. Pour ce $I$, on trouve

$$\det A_I = \begin{vmatrix} 0 & & & -a_{n-k} \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{vmatrix} = (-1)^k a_{n-k} \text{ comme voulu.}$$

Deuxième étape : un petit calcul où l'on casse une partie $K \subset \{1,\ldots,a+b\}$ en une partie $I \subset \{1,\ldots,a\}$ jointe

à une partie $J \subset \{1,...,b\}$. On note $a$ et $b$ les tailles de $A$ et $B$ :

$$\begin{aligned} D\begin{pmatrix} A & \\ & B \end{pmatrix} &= \sum_{K\subset\{1,...,a+b\}} \det\left[\begin{pmatrix} A & \\ & B \end{pmatrix}_K\right] t^{a+b-|K|} \\ &= \sum_{I,J} \det A_I \ \det B_J \ t^{a+b-|I\cup J|} \\ &= \sum_{I,J} (\det A_I)\, t^{a-|I|} \ \ (\det B_J)\, t^{b-|J|} \\ &= \sum_{I} (\det A_I)\, t^{a-|I|} \sum_{J} (\det B_J)\, t^{b-|J|} \\ &= D(A)\, D(B)\,. \end{aligned}$$

Troisième étape : on se rappelle que $GL_n$ est engendré par les transvections et les dilatations. Il suffit donc de vérifier que chacun des coefficients $\sum_{|I|=k} \det A_I$ du polynôme $D(A)$ est invariant par l'action sur $A$ (par conjugaison) d'une transvection ou une dilatation.

Or, lorsque l'on dilate la $i$-ième ligne/colonne de $A$ par un scalaire $\lambda$, l'opération se répercute de la même manière sur $A_I$ si $i \in I$, ce qui fait sortir un $\lambda$ quand on prend le déterminant. Mais on conjugue, donc il sort aussi un scalaire $\frac{1}{\lambda}$ qui vient tuer le premier. Dans le cas où $i \notin I$, les dilatations ne touchent pas à $A_I$, donc le déterminant est inchangé dans tous les cas.

Le même raisonnement tient (presque) pour les transvections. Lorsqu'on fait agir une transvection $I_n + \alpha E_{i,j}$ sur $A$, on fait une opération sur les lignes/colonnes de $A$, laquelle opération se répercute sur les lignes/colonnes de $A_I$ (évidemment, si $i$ et $j$ sont hors de $I$, $A_I$ est inchangée) ; en particulier, la nouvelle matrice extraite $A_I$ est obtenue à partir de l'ancienne par une opération de transvection si $i$ et $j$ sont tous deux dans $I$, ce qui ne change pas son déterminant. Évidemment, la conjugaison étant deux multiplications successives, conjuguer par une transvection ne change pas nos $\det A_I$. Il reste à voir le cas où exactement un des indices $i, j$ est dans $I$ : en effet, lorsqu'on extrait $A_I$, on emporte avec soi la ligne/colonne dont on aimerait disposer pour opérer la transvection en sens inverse. Qu'à cela ne tienne, on va la rajouter pour pouvoir faire ce qu'on veut. Détaillons cela.

Notons $A'$ la conjuguée de $A$ par la dilatation $I+\alpha E_{i,j}$ : on applique à $A$ les opérations $\begin{cases} L_i \longleftarrow L_i + \alpha L_j \\ C_j \longleftarrow C_j - \alpha C_i \end{cases}$. Considérons à présent une partie $I$ de cardinal $k$ contenant $i$ mais pas $j$. On a clairement une partie "duale" $I^*$ où l'on a remplacé $i$ par $j$. Montrons que $\det A_I + \det A_{I^*}$ est inchangé par la conjugaison considérée. Les autres déterminant extraits mettant restant inchangés d'après les remarques préliminaires, on aura gagné.

Explicitons les indices de $I$ :

$$I = \{i_1 < i_2 < ... < i_\nu < ... < i_k\} \text{ où } \nu \text{ est la place de } i = i_\nu.$$

On calcule $\det A_I$ en rajoutant la ligne manquante ($L_j$ indicée par $I$) pour revenir en arrière :

$$\begin{aligned} \det A_I &= \begin{vmatrix} a_{i_1,i_1} & \cdots & a_{i_1,i_k} \\ \vdots & & \vdots \\ a_{i_\nu,i_1} + \alpha a_{j,i_1} & \cdots & a_{i_\nu,i_k} + \alpha a_{j,i_k} \\ \vdots & & \vdots \\ a_{i_k,i_1} & \cdots & a_{i_k,i_k} \end{vmatrix} = \begin{vmatrix} 1 & a_{j,i_1} & \cdots & a_{j,i_k} \\ 0 & & & \\ \vdots & & A'_I & \\ 0 & & & \end{vmatrix} = \begin{vmatrix} 1 & a_{j,i_1} & \cdots & a_{j,i_k} \\ 0 & & & \\ \vdots & & & \\ -\alpha & & A_I & \\ \vdots & & & \\ 0 & & & \end{vmatrix} \\ &= \det A_I - (-1)^\nu \,\alpha \det \begin{pmatrix} L'_j \\ L'_{i_1} \\ \vdots \\ L'_{i_k} \end{pmatrix} \text{ où il manque la } \nu\text{-ième ligne } L'_i \text{ de } A'_I \\ &= \det A_I + \alpha \det \begin{pmatrix} L'_{i_1} \\ \vdots \\ L'_{i_k} \end{pmatrix} \text{ où la ligne } L'_i \text{ est remplacée par la ligne } L'_j. \end{aligned}$$

Le même calcul tient pour $\det A_{I^*}$ : on tranpose la matrice pour avoir exactement la même situation, à une transposition $(i, j)$ près et à un signe devant le $\alpha$ :

$$\det A_{I^*} = \det A_I - \alpha \det\left(C'_{i_1}, ..., C'_{i_k}\right) \text{ où la colonne } C'_j \text{ est remplacée par } C'_i.$$

Il reste à remarquer que les deux matrices perturbatrices qui apparaissent sont en fait les mêmes : on extrait de $A$ les lignes d'indice $\in I$ et les colonnes d'indice $\in I^*$.

Appliqué au polynôme caractéristique, on trouve ainsi

$$\chi_A = \sum_{k=0}^{n} (-1)^k \left( \sum_{|I|=k} \det A_I \right) X^{n-k}.$$

Pour $k = 0$, la contribution est celle du déterminant de la matrice vide, lequel vaut 1, et on retrouve que $\chi_A$ est unitaire. Pour $k = 1$, on retrouve le coefficient sous-dominant $-\operatorname{tr} A$ et pour $k = n$ on retrouve le terme constant $(-1)^k \det A$.

**Remarque.** On peut également obtenir le résultat par un calcul direct (cf. feuille sur les déterminants) ou encore en trigonalisant (cf. feuille 1 sur la réduction).