Décomposition de Frobenius

I - Sous-espace stable et endo cyclique
II - Décomposition de Frobenius
III - Calcul pratique
IV - Application.

Réf: Gourdon, Algèbre (p289)
Algèbre & grand combat (p 101-3)

On considère E un $\mathbb{K}$-ev de dim finie n et $f \in \mathcal{L}(E)$.

I - Sous-espace stable et endo cyclique:

Définitions: . On note π_f le pol min de f et $\mathcal{L}(f) = \{P(f) \mid P \in \mathbb{K}[X]\}$.

. Pour $x \in E$, on note P_x le pol engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et $E_x = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$.

Proposition: . Si $k = \deg(\pi_f)$ alors $\mathcal{L}(f)$ est un s.e.v de $\mathcal{L}(E)$ de dimension k et dont une base est $(Id, f, \dots, f^{k-1})$.

. si $\ell = \deg(P_x)$ alors E_x est un s.e.v de E de dimension ℓ, dont une base est $(x, \dots, f^{\ell-1}(x))$.

Preuve: On a l'application linéaire $ev_f : \mathbb{K}[X] \longrightarrow \mathcal{L}(E)$ et $\ker(ev_f) = \langle \pi_f \rangle$.
$P \longmapsto P(f)$ $\quad \mathrm{Im}(ev_f) = \mathcal{L}(f)$.

Ainsi ev_f induit un isomorphisme $\widetilde{ev}_f : \mathbb{K}[X]/\langle \pi_f \rangle \xrightarrow{\sim} \mathcal{L}(f)$.
Or $(1, \bar{X}, \dots, \bar{X}^{k-1})$ est une base de $\mathbb{K}[X]/\langle \pi_f \rangle$ ainsi $\widetilde{ev}_f$ étant un isomorphisme, $(Id, f, \dots, f^{k-1})$ est une base de $\mathcal{L}(f)$. Car on a le diagramme suivant:

$$\begin{array}{ccc} \mathbb{K}[X] & \xrightarrow{ev_f} & \mathcal{L}(f). \\ \pi \downarrow & \circlearrowleft & \nearrow \widetilde{ev}_f \\ \mathbb{K}[X]/\langle \pi_f \rangle & & \end{array} \qquad \text{donc } ev_f = \widetilde{ev}_f \circ \pi.$$

De même pour l'autre partie avec:

$$\begin{array}{ccc} \mathbb{K}[X] & \xrightarrow{ev_{x,f}} & E_x \\ \pi \downarrow & & \nearrow \widetilde{ev}_{x,f} \\ E_x & & \end{array} \qquad \text{où } ev_{x,f} : \mathbb{K}[X] \longrightarrow E_x, \; P \longmapsto P(f)(x).$$

□

Lemme : 1) Soient $x_1, \dots, x_p$ tq $E_{x_1}, \dots, E_{x_p}$ soient en somme directe alors $P_{x_1+\dots+x_n} = \text{ppcm}(P_{x_1}, \dots, P_{x_n})$.

2) Soient $x_1, \dots, x_p$ tq $P_{x_1}, \dots, P_{x_p}$ soient premier entre eux alors $E_{x_1+\dots+x_n} = \bigoplus_{i=1}^{p} E_{x_i}$.

p 178.

Preuve : 1) On montre le cas pour $p=2$, et on conclut par récurrence. On considère donc $x, y \in \mathcal{L}$ tq $E_x \cap E_y = \{0\}$.

Mq : $P_x \mid P_{x+y}$ et $P_y \mid P_{x+y}$.

Par cela on remarque que :

$$0 = P_{x+y}(f)(x+y) \quad \text{donc} \quad \underbrace{P_{x+y}(f)(x)}_{\in E_x} = -\underbrace{P_{x+y}(f)(y)}_{\in E_y} \in E_x \cap E_y = \{0\}$$

donc

$$P_{x+y}(f)(x) = P_{x+y}(f)(y) = 0$$

D'où $P_x \mid P_{x+y}$ et $P_y \mid P_{x+y}$.

Soit Q tel que $P_x \mid Q$ et $P_y \mid Q$ alors

$$Q(f)(x+y) = \underbrace{Q(f)(x)}_{=0} + \underbrace{Q(f)(y)}_{=0} = 0$$

Donc $P_{x+y} \mid Q$, d'où le résultat.

2) Soit $z \in E_x \cap E_y$ alors $P_x(z) = 0$ et $P_y(z) = 0$

donc $P_z \mid P_x$ et $P_z \mid P_y$.

i.e $P_z \mid \text{pgcd}(P_x, P_y) = 1$ donc $P_z = 1$ donc $z = 0$ donc $E_x \cap E_y = \{0\}$.

$\Downarrow$

$P_{x+y} = \text{ppcm}(P_x, P_y) = P_x P_y$

$\Downarrow$

$\dim E_{x+y} = \dim E_x + \dim E_y$.

Soit $P \in \mathbb{K}[X]$ alors $P(f)(x+y) = P(f)(x) + P(f)(y)$

donc $E_{x+y} \subset E_x \oplus E_y$.

Soit $z = L(f)(x) + Q(f)(y) \in E_x \oplus E_y$. Il existe $U, V \in \mathbb{K}[X]$ tel que

$$P_x U + P_y V = 1.$$

Alors $H = QP_xU + LP_yV$, alors

$$H(f)(x+y) = Q(f) \circ \underbrace{\left(P_x U(f)\right)}_{=0}(x+y) + L(f) \circ (P_y V)(x+y) = Q(f)(y) + L(f)(x) = z$$

car $P_x U(f)(x+y) = U\widetilde{P_x(f)}(x) + UP_x(f)(y) = y - VP_y(f)(y) = y$.

$P_y V(f)(x+y) = x$

donc $E_x \oplus E_y \subset E_{x+y}$

□

Proposition : Il existe $x \in E$ tel que $P_x = \Pi_f$. (p178)

Preuve : Soit M un facteur irréductible de Π_f et α sa multiplicité.
Alors $\Pi_f = M^\alpha N$ avec $M^\alpha \wedge N = 1$ ainsi par le lemme des noyaux :

$$E = \ker(M^\alpha(f)) \oplus \ker(N(f)).$$

Soit $x \in \ker(M^\alpha(f))$ alors $M^\alpha(f)(x) = 0$ donc $P_x \mid M^\alpha$.

donc $P_x = M^{\beta_x}$ où $\beta_x \leq \alpha$ car M irréductible.

Par l'absurde supposons que pour tout $x \in \ker M^\alpha(f)$, $\beta_x < \alpha$.

Alors

$$\forall x \in \ker M^\alpha(f),\ P_x \mid M^{\alpha-1} \text{ donc } \ker M^\alpha(f) \underset{\text{stab}}{=} \ker M^{\alpha-1}(f)$$

Donc

$$E = \ker M^{\alpha-1}(f) \oplus \ker N(f).$$

Soit $\vec{z} = \vec{x} + \vec{y}$ alors

$$M^{\alpha-1}N(f)(z) = N(f) \circ M^{\alpha-1}(f)(x) + M^{\alpha-1}(f) \circ N(f)(y) = 0$$

donc $\Pi_f \mid M^{\alpha-1}N$ absurde.

Ainsi il existe $x \in \ker M^\alpha(f)$ tel que $P_x = M^\alpha$.

On écrit donc $\Pi_f = \prod_{i=1}^{d} M_i^{\alpha_i}$ et $x_i \in \ker M_i^{\alpha_i}(f)$ tq $P_{x_i} = M_i^{\alpha_i}$. Ainsi $P_{x_1}, \dots, P_{x_d}$ premiers entre eux donc :

$$P_{x_1+\dots+x_d} = P_{x_1} \oplus \dots \oplus P_{x_d}$$

Par le lemme $P_{x_1+\dots+x_d} = \text{ppcm}(M_i^{\alpha_i}) = \prod_{i=1}^{d} M_i^{\alpha_i} = \Pi_f$.

∎

Définition : Endomorphisme cyclique.
On dit que $f \in \mathcal{L}(E)$ est cyclique s'il existe $x \in E$ tel que $P_x = E$. Ce qui est équivalent à dire que $\deg(\Pi_f) = n$ ou que $\Pi_f = \chi_f$.

Définition : Soit $P = X^p + a_{p-1}X^{p-1} + \dots + a_0 \in \mathbb{K}[X]$. On appelle matrice compagnon de P la matrice :

$$C(P) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \\ & & 1 & -a_{n-1} \end{pmatrix} \in \mathcal{M}_p(\mathbb{K})$$

Ainsi $\chi_{C(P)} = P$.

Proposition : Soit f un endomorphisme cyclique. Il existe une base de E dans laquelle la matrice de f soit égale à $C(\pi_f)$.

Preuve : Comme f est cyclique il existe x tel que $E_x = E$. Alors $P_x = \pi_f$ et $(x, f(x), \dots, f^{n-1}(x)) = \mathcal{B}$ est une base de E ainsi dans cette base :

$$\mathrm{Mat}_{\mathcal{B}}(f) = C(P_x) = C(\pi_f).$$

Car $\pi_f(f)(x) = 0$.

II - Décomposition de Frobenius

On peut maintenant énoncer le théorème de la réduction de Frobenius.

Théorème : Soit $f \in \mathcal{L}(E)$. Il existe une suite $F_1, \dots, F_r$ de s.e.v de E, stables par f, telle que :

1) $E = F_1 \oplus \dots \oplus F_r$
2) Pour $i \in [\![1, r]\!]$, $f_i = f|_{F_i}$ est un endomorphisme de F_i cyclique.
3) Si P_i désigne le pol minimal de f_i, on a $P_{i+1} | P_i$.

La suite $P_1, \dots, P_r$ ne dépend que de f et non de la décomposition $F_1, \dots, F_r$. On l'appelle suite des invariants de similitude de f et $P_1 = \pi_f$, $P_1 \dots P_r = \chi_f$.

Preuve : Existence :

On procède par récurrence forte sur n.

Si $n = 1$: ok

Si $n \geq 1$: On suppose le résultat vrai pour tout $k \leq n$.

Objectif : On veut écrire $E = F \oplus G$ avec F, G stable par f et $f|_F$ cyclique.

Par cela on écrit $k = \deg(\pi_f)$ et on considère $x \in E$ tel que $P_x = \pi_f$.
Soit $F = E_x$ qui est un s.e.v de E de dim k, stable par f (par définition) Et comme $\deg(P_x) = \deg(\pi_f) = k$ on sait qu'une base de F est :

$$e_1 = x, e_2 = f(x), \dots, e_k = f^{k-1}(x).$$

Ainsi $f|_F$ est cyclique.
On complète la base en $(e_1, \dots, e_n)$ une base de E et on note $(e_1^*, \dots, e_n^*)$ la base dual. On note ainsi :

$$G = \{y \in E \mid \forall \varphi \in \Gamma, \varphi(y) = 0\} \text{ où } \Gamma = \text{Vect}\left({}^t f^i(e_k^*), i \in \mathbb{N}\right) = \text{Vect}\left(e_k^* \circ f^i, i \in \mathbb{N}\right).$$

Alors G est un s.e.v de E.
G est f stable car pour $y \in G$, $i \in \mathbb{N}$.

$$e_k^* \circ f^i(f(y)) = e_k^* \circ f^{i+1}(y) = 0$$

donc $f(y) \in G$
Montrons que $F \oplus G = E$ i.e $F \cap G = \{0\}$ et $\dim(F) + \dim(G) = n$.
Soit $y \in F \cap G$, $y \neq 0$ alors on peut écrire $y = a_1 e_1 + \dots + a_p e_p$ avec $a_p \neq 0$ et $p \leq k$. Or $y \in G$ ainsi en composant par $e_p^* \circ f^{k-p}$ on a :

$$0 = e_k^*(a_1 e_{k-p+1} + \dots + a_p e_k) = a_p.$$

ce qui est absurde. $F \cap G = \{0\}$.
On sait que $\dim F = k$, il nous suffit de montrer que $\dim G = n - k$ or $G = \Gamma^\circ$, il suffit de montrer que $\dim(\Gamma) = k$.
Pour cela on considère l'application linéaire.

$$\varphi : \mathcal{L}(f) = \{P(f) \mid P \in \mathbb{K}[X]\} \longrightarrow \Gamma$$
$$g \longmapsto e_k^* \circ g.$$

Il est clair que φ est surjective.
De plus φ est injective, en effet si $e_k^* \circ g = 0$ avec $g \neq 0$, $g = a_1 \text{Id}_E + \dots + a_p f^{p-1} \in \mathcal{L}(f)$
$a_p \neq 0$ et $p \leq k$.

$$0 = e_k^* \circ g(f^{k-p}(x)) = e_k^*(a_1 \underbrace{f^{k-p}(x)}_{e_{k-p}} + \dots + a_p \underbrace{f^{k-1}(x)}_{e_k}) = a_p \neq 0.$$

Ainsi φ est un isomorphisme donc $\dim \Gamma = \dim \mathcal{L}_f = k$.

On a donc $E = F \oplus G$ avec F, G f stable et $f|_F$ cyclique.

Si on note P_1 le polynôme minimale de $f|_F$, alors $P_1 = P_x = \pi_f$ et P_2 le polynôme minimal de $f|_G$.
Comme G est f stable, $\pi_f(f|_G) = P_1(f|_G) = 0$ donc $P_2 | P_1$.
On applique par récurrence le résultat à G, $f|_G$ et on obtient le résultat voulue.

Unicité: On note $f_1, .., f_r$ et $G_1, ..., G_s$ vérifiant le théo et $P_i = \pi_{f|_{f_i}}$, $Q_j = \pi_{f|_{G_j}}$.
On a $P_1 = \pi_f = Q_1$.
On raisonne par l'absurde en supposant les listes différents, ainsi comme:

$$\sum_{i=1}^{r} \deg(P_i) = n = \sum_{j=1}^{s} \deg(Q_j)$$

On peut noter j le premier indice tel que $P_j \neq Q_j$.
On sait que $E = f_1 \oplus \dots \oplus f_r$, avec f_i, f-stables et $P_j(f)(f_k) = \{0\}$ pour $k \geq j$ ainsi:

① $P_j(f)(E) = P_j(f)(f_1) \oplus \dots \oplus P_j(f)(f_{j-1})$

Et par ailleurs, $E = G_1 \oplus \dots \oplus G_s$, qui sont f stables donc:

② $P_j(f)(E) = P_j(f)(G_1) \oplus \dots \oplus P_j(f)(G_{j-1}) \oplus P_j(f)(G_j) \oplus \dots \oplus P_j(f)(G_s)$

Pour $k \in [\![1, j-1]\!]$, comme f_k est cyclique sur F_k et G_k il existe des bases B_F et B_G tel que:

$$\underset{B_F}{Mat}(f|_{F_k}) = C(P_k) = C(Q_k) = \underset{B_G}{Mat}(f|_{G_k})$$

($k \leq j-1$)
Ainsi $P_j(f|_{F_k})$ et $P_j(f|_{G_k})$ ont même rang.
Donc $\dim P_j(f)(F_k) = \dim P_j(f)(G_k)$, ainsi en prenant les dim dans ① et ②, on obtient que:

$$\sum_{k=j}^{s} \dim(P_j(f)(G_k)) = 0$$

$$\dim P_j(f)(G_j) = \dots = \dim P_j(f)(G_s) = 0$$

En particulier $P_j(f|_{G_j}) = 0$ donc $Q_j | P_j$.
Par symétrie, $P_j | Q_j$ ainsi $Q_j = P_j$, car unitaires, ce qui est absurde.
Ainsi $\forall j \leq \min(r, s)$, $P_j = Q_j$ or $\sum \deg(P_j) = n = \sum \deg(Q_j)$ donc $r = s$ d'où le résultat.

Sous forme matricielle ceci donne le théorème suivant.

Théorème: Soit $f \in \mathcal{L}(E)$ et $P_1, .., P_r$ ses invariants de similitude alors il existe B une base de E telle que:

$$\underset{B}{Mat}(f) = \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix}$$

Par ailleurs, $P_1 = \pi_f$ et $\chi_f = P_1 \dots P_r$.

Preuve: Pour F_i, $f|_{F_i}$ est cyclique donc en prenant des bases adaptées, comme $E = \bigoplus_{i=1}^{r} F_i$ on a le résultat en concaténant les bases.

□

Corollaire: Soit $f, g \in \mathcal{L}(E)$ alors f et g sont semblables si et seulement si ils ont les mêmes invariants de similitude.

Preuve: $\Leftarrow$ Si f et g ont les mêmes invariants de similitude alors il existent des bases $\mathcal{B}$ et $\mathcal{B}'$ tel que:

$$\mathcal{M}at_{\mathcal{B}}(f) = \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix} = \mathcal{M}at_{\mathcal{B}'}(g).$$

d'où f et g sont semblables.

$\Rightarrow$ Soit f, g semblables alors il existe $P \in GL_n(\mathbb{K})$ et $P_1, \dots, P_r$ les invariants de similitudes de f tel que:

$$P\,\mathcal{M}at_{\mathcal{B}}(g)\,P^{-1} = \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix}$$

i.e $\mathcal{M}at_{\mathcal{B}'}(g) = \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix}$ où $\mathcal{B}'$ une base de E.

Par unicité des invariants de similitudes, $P_1, \dots, P_r$ sont les invariants de similitudes de f.

□

Corollaire: Soient $k \subset K$ deux corps et $M \in \mathcal{M}_n(k)$. Les invariants de similitude de $M \in \mathcal{M}_n(k)$ sont aussi les invariants de similitudes de $M \in \mathcal{M}_n(K)$.

De plus si $U, V \in \mathcal{M}_n(k)$ alors:

U et V semblables dans $\mathcal{M}_n(k) \iff U$ et V semblables dans $\mathcal{M}_n(k)$

Preuve: On sait qu'il existe $P \in GL_n(k)$ telle que

$$PMP^{-1} = \begin{bmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{bmatrix}$$

où $P_r | \dots | P_1$ sont les invariants de similitudes.

Or $k \subset K$ donc $P \in GL_n(K)$ et $P_r | \dots | P_1$ dans $K[X]$ ainsi par unicité du théorème. $P_1, \dots, P_r$

sont les invariants de similitudes de $M \in \mathcal{M}_n(K)$.
Le deuxième point est direct par le corollaire précédent. ∎

Remarque Si A et B sont deux anneaux, $A \subset B$ on a seulement :

$$U, V \text{ semblables dans } \mathcal{M}_n(A) \Rightarrow U, V \text{ semblables dans } \mathcal{M}_n(B)$$

Un autre exemple est $A = \mathbb{Z}$, $B = \mathbb{Q}$ avec

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } V = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Semblables sur $\mathbb{Q}$ car $\widehat{m}$ pol caractéristique $X^2 - 1 = (X-1)(X+1)$ et diagonalisable.
Mais pas $\mathbb{Z}$, voir réduction modulo $\mathbb{Z}/2\mathbb{Z}$.

Application: Classes de similitude en dimension 2 et 3.
On a : u, v semblables $\iff \pi_u = \pi_v$ et $\chi_u = \chi_v$.
Dim 2: u a au plus 2 invariants de similitudes P_1 et P_2 or $P_1 = \pi_u$ et $P_1 P_2 = \chi_u$
donc $P_2 = \frac{\chi_u}{\pi_u}$ ainsi π_u et χ_u déterminent entièrement les deux.
Dim 3: u a au plus 3 invariants de similitudes.
Si $\deg(\pi_u) = 3$ alors $\pi_u = \chi_u$ donc u à un seul invariants π_u.
Si $\deg(\pi_u) = 2$ alors $P_1 = \pi_u$ et $P_2 P_3 = \frac{\chi_u}{\pi_u}$ de degré 1 donc $P_2 = 1$ ou $P_3 = 1$ i.e u a 2 invariants entièrement déterminé par π_u et χ_u.
Si $\deg(\pi_u) = 3$ alors $\pi_u = X - \lambda$ donc u est une homothéties et ses invariants sont (π_u, π_u, π_u) d'où le résultat.

IV - Calcul pratique :

On va utiliser la forme de smith de la matrice $XI_n - M$ dans $\mathbb{K}[X]$ pour calculer les invariants de similitudes de M.
On commence par la proposition suivante qui fait le lien dans un sens.

Proposition: Soit $f \in \mathcal{L}(E)$ et M sa matrice dans une base de E fixée. Soit $F_1, \dots, F_r$ une décomposition de Frobenius de f, $E = F_1 \oplus \dots \oplus F_r$.
En notant $P_i = \pi_{f|_{F_i}}$ les invariants de similitude de f alors $XI_n - M$ et $\mathbb{K}[X]$-équivalente à

$$\begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix}$$

De plus $n-r+1 = \min\left\{ j \in [\![1,m]\!] \,\middle|\, \mu_j(XI_m - M) \neq 1 \right\}$ et

$$P_i = \frac{\mu_{n-r+i}(XI_m - M)}{\mu_{n-r+i-1}(XI_m - M)} \quad \forall i \in [\![1,r]\!].$$

où $\mu_j(XI_m - M)$ est le pgcd unitaire des j-mineurs de $XI_m - M$ (avec la convention $\mu_0(XI_n - M) = 1$).

Preuve : Dans une bonne base $\mathcal{B}$ on a :

$$Mat_{\mathcal{B}}(f) = \begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix} =: C$$

Il existe donc $P \in GL_n(\mathbb{K})$ telle que $P^{-1}MP = C$, ainsi :

$$P^{-1}(XI_n - M)P = \begin{pmatrix} XId_1 - C_{P_1} & & \\ & \ddots & \\ & & XId_r - C_{P_r} \end{pmatrix}$$

Ainsi si on suppose le résultat vrai pour les matrices compagnons, il existe $S_i, T_i \in GL_{d_i}(\mathbb{K}[X])$ tel que :

$$S_i(XId_i - C_{P_1})T_i = \begin{pmatrix} I_{d_i-1} & \\ & P \end{pmatrix} \quad \forall i \in [\![1,r]\!].$$

Alors avec $S = \begin{pmatrix} S_1 & & \\ & \ddots & \\ & & S_r \end{pmatrix}$, $T = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_r \end{pmatrix}$ on a :

$$S(XI_m - C)T = \begin{pmatrix} Id_{d_1-1} & & & \\ & P_1 & & \\ & & \ddots & \\ & & & Id_{r-1} P_r \end{pmatrix}$$

En changeant l'ordre des vecteurs dans la base i.e multiplier par un produit de matrices de transpositions convenables, on obtient une matrice $Q \in GL_n(\mathbb{K})$ tel que :

$$\underbrace{QSP^{-1}}_{U \in GL_n(\mathbb{K}[X])}(X_n - M)\underbrace{PT}_{V \in GL_n(\mathbb{K}[X])} = \begin{pmatrix} Id_{n-r} & & \\ & P_1 & \\ & & P_r \end{pmatrix}$$

Il nous reste à montrer le résultat pour les matrices compagnons.
Soit $P = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{K}[X]$, et C_P sa matrice compagnon alors :

$$XI_n - C(P) = \begin{pmatrix} X & & & a_0 \\ -1 & \ddots & & \vdots \\ & \ddots & X & a_{n-2} \\ & & -1 & X+a_{n-1} \end{pmatrix}$$

Si on fait l'opération $L_1 \leftarrow L_1 + XL_2 + \dots + X^{n-1}L_n$ (qui est une succession d'opérations élémentaires) on a:

$$XI_n - C(P) \sim \begin{pmatrix} 0 & \cdots & 0 & P \\ -1 & X & & a_1 \\ & \ddots & \ddots & \vdots \\ & & X & \\ & & -1 & X+a_{n-1} \end{pmatrix}$$

On effectue $C_j \leftarrow C_j + XC_{j-1}$ pour $j \in [\![1, n-1]\!]$, on obtient:

$$XI_n - C(P) \sim \begin{pmatrix} 0 & & & P \\ -1 & \ddots & & a_1 \\ & \ddots & 0 & \vdots \\ & & -1 & a_{n-1} \end{pmatrix}$$

Finalement, on fait $C_n \leftarrow a_1C_1 + a_2C_2 + \dots + a_{n-1}C_{n-1} + C_n$ on montre que:

$$XI_n - C(P) \sim \begin{pmatrix} 0 & & & P \\ -1 & \ddots & & 0 \\ & \ddots & 0 & \vdots \\ & & -1 & 0 \end{pmatrix}$$

En changeant les lignes et les colonnes on obtient que $XI_n - C(P)$ est $\mathbb{K}[X]$-équivalente à $\begin{pmatrix} I_{n-1} & \\ & P \end{pmatrix}$ d'où le résultat.

Le dernier point vient du théorème sur la réduction de Smith dans un anneau (p575 de Algèbre le grand combat).

■

Grâce à la proposition on peut calculer, grâce à smith, les invariants de similitudes. On s'intéresse maintenant à l'obtention pratique d'une base de Frobenius adaptée à f. On redémontrera au passage l'existence.

Lemme: Soit $f \in \mathcal{L}(E)$ et $B = (e_1, \dots, e_n)$ une base de E.

Soit $M = Mat_{\mathcal{B}}(f)$ et $C_1, \dots, C_n$ les colonnes de la matrice $XI_n - M \in \mathcal{M}_n(\mathbb{K}[X])$. Alors l'application linéaire,

$$\varphi : \mathbb{K}[X]^n \longrightarrow E$$
$$\begin{pmatrix} P_1 \\ P_n \end{pmatrix} \longmapsto P_1(f)(e_1) + \dots + P_n(f)(e_n).$$

est surjective et $\ker(\varphi) = \{ Q_1 C_1 + \dots + Q_n C_n \mid Q_1, \dots, Q_n \in \mathbb{K}[X] \} = \underset{\mathbb{K}[X]\text{-module}}{\text{Vect}}(C_1, \dots, C_n)$.

Preuve :

Il est clair que φ est linéaire, et que e_i est dans l'image de φ $(\forall i)$ d'où la surjectivité de φ.

Montrons que $C_1, \dots, C_n \in \ker(\varphi)$, en effet on a :

$$\varphi(C_j) = \sum_{i=1}^{n} (\delta_{ij} X - a_{ij})(u)(e_i) = \sum_{i=1}^{n} (\delta_{ij} u(e_i) - a_{ij} e_i) = u(e_j) - \sum_{i=1}^{n} a_{ij} e_i = 0.$$

$\hookrightarrow$ def de M.

Or φ étant $\mathbb{K}[X]$-linéaire, $\{ Q_1 C_1 + \dots + Q_n C_n \mid Q_1, \dots, Q_n \in \mathbb{K}[X] \} \subset \ker(\varphi)$.

Soit maintenant $v = \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} \in \ker(\varphi)$.

On fait une récurrence sur $d := \max(\deg P_i)$, par montrer de $\begin{pmatrix} P_1 \\ P_n \end{pmatrix}$ est une combinaison linéaire des $C_1, \dots, C_n$.

Si $d = 0$, $P_1, \dots, P_n$ sont constants alors

$$0 = \sum P_i(f)(e_i) = \sum a_i e_i \Rightarrow a_1 = \dots = a_n = 0 \text{ (base)}$$

donc OK

Si $d \geq 1$, on suppose le résultat vrai pour $k \leq d$.

On fait la division euclidienne de P_i par $X - a_{ii}$. On a donc :

$$P_i = (X - a_{ii}) \underbrace{Q_i}_{\deg \leq d-1} + \underbrace{r_i}_{\in \mathbb{K}}.$$

Or par $\mathbb{K}[X]$-linéarité, $v - \sum_{j=1}^{n} Q_j C_j \in \ker(\varphi)$. Or on a :

$$v_i = P_i - \sum_{j=1}^{n} (\delta_{ij} X - a_{ij}) Q_j = P_i - (X - a_{ii}) Q_i + \sum_{i \neq j} a_{ij} Q_j = r_i + \sum_{i \neq j} a_{ij} Q_j$$

donc $\deg(v_i) \leq d - 1$, donc par hypothèse de récurrence on a le résultat. ∎

Corollaire: Soient $U, V \in GL_n(\mathbb{K}[X])$ telles que:

$$U(XI_n - M)V = \begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix}$$

où $P_1, \dots, P_r$ sont unitaires non constants et $P_1 | \dots | P_r$.
Soient $Y_1, \dots, Y_r \in \mathbb{K}[X]^n$ les r dernières colonnes de U^{-1}. Posons

$$Y_j = \begin{pmatrix} R_{1j} \\ \vdots \\ R_{nj} \end{pmatrix}, \forall j \in [\![1, r]\!].$$

et posons

$$v_j = \sum_{i=1}^{n} R_{ij}(u)(e_i), \forall j \in [\![1, r]\!].$$

Pour tous $Q_1, \dots, Q_r \in \mathbb{K}[X]$, on a:

$$Q_1(f)(v_1) + \dots + Q_r(f)(v_r) = 0 \Rightarrow P_j | Q_j, \forall j \in [\![1, r]\!].$$

Preuve:

Soient $Q_1, \dots, Q_r$ vérifiant:

$$Q_1(f)(v_1) + \dots + Q_r(f)(v_r) = 0.$$

Par définition des v_j cela donne:

$$0 = \sum_{j=1}^{r} \sum_{i=1}^{n} Q_j(u)\left(R_{ij}(u)(e_i)\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{r} (Q_j R_{ij})(u) \right)(e_i) = 0$$

Or si on note $Z_1, \dots, Z_{n-r}, Y_1, \dots, Y_r \in \mathbb{K}[X]^n$ désignant les colonnes de U^{-1}, cette égalité se retraduit par:

$$\varphi(Q_1 Y_1 + \dots + Q_r Y_r) = 0.$$

Ainsi d'après le lemme, $Q_1 Y_1 + \dots + Q_r Y_r$ est une combinaison linéaire des $C_1, \dots, C_r$, les colonnes de $XI_n - M$.
Or remarquons que les colonnes de la matrice

$$U^{-1} \begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix} V^{-1} \text{ sont } Z_1, \dots, Z_{n-r}, P_1 Y_1, \dots, P_r Y_r.$$

Or on sait que $XI_n - M = U^{-1} \begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix} V^{-1}$.

Ainsi $C_1, \dots, C_n$, les colonnes de $XI_n - M$ sont des combinaisons $\mathbb{K}[X]$-linéaires de $Z_1, \dots, Z_{n-r}$, $P_1 Y_1, \dots, P_r Y_r$.
Il existe donc des polynômes $S_1, \dots, S_{n-r}, T_1, \dots, T_r \in K[X]$ tels que:

$$Q_1 Y_1 + \dots + Q_r Y_r = S_1 Z_1 + \dots + S_{n-r} Z_{n-r} + T_1 P_1 Y_1 + \dots + T_r P_r Y_r.$$

Or U est inversible dans $\mathcal{M}_n(\mathbb{K}[X])$ donc dans $\mathcal{M}_n(\mathbb{K}(X))$ donc ses colonnes sont $K(X)$-linéairement indépendantes. Ainsi

$$\forall i,\ Q_i = T_i P_i \Rightarrow P_i \mid Q_i$$

□

On peut conclure avec la méthode explicite.

Proposition: Soit E un K-espace vectoriel de dimension $n \geq 1$, et soit $u \in \mathcal{L}(E)$. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et soit $M = Mat_{\mathcal{B}}(u)$.
Soient $U, V \in GL_n(K[X])$ donc matrices telles que:

$$U(XI_n - M)V = \begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix}$$

où $P_1, \dots, P_r \in K[X]$ sont unitaires non constants et vérifient les relations de divisibilité $P_1 \mid P_2 \mid \dots \mid P_r$.
Soient $Y_1, \dots, Y_r \in K[X]^n$ les r dernières colonnes de U^{-1}. On pose:

$$Y_j = \begin{pmatrix} R_{1j} \\ \vdots \\ R_{nj} \end{pmatrix}, \quad \forall j \in [\![1, r]\!].$$

et posons

$$v_j = \sum_{i=1}^{n} R_{ij}(u)(e_i), \quad \forall j \in [\![1, r]\!].$$

Soit $d_j = \deg(P_j)$ et soit $F_j = Vect_K(v_j, u(v_j), \dots, u^{d_j - 1}(v_j))$ alors:

$$E = F_1 \oplus \dots \oplus F_r$$

est une décomposition de Frobenius de u, et le polynôme minimal de $u_{|F_j}$ est égal à P_j.
En particulier, $P_1, \dots, P_r$ sont les invariants de similitude de u.

Preuve: Montrons que la famille :

$$B_f = (v_1, u(v_1), \dots, u^{d_1-1}(v_1), \dots, v_r, u(v_r), \dots, u^{d_r-1}(v_r))$$

est libre.
Une combinaison K-linéaire est exactement des éléments de E de la forme :

$$Q_1(u)(v_1) + \dots + Q_r(u)(v_r)$$

où $\deg(Q_i) < d_i \quad \forall i \in [\![1, r]\!]$.
D'après le corollaire si la combinaison K-linéaire est nulle alors $P_i \mid Q_i$ or $\deg(P_i) = d_i$
Ainsi $\deg(Q_i) < d_i$

$$Q_1 = \dots = Q_r = 0$$

La famille est libre.
Pour démontrer que c'est une base il suffit de voir quel est de cardinal n i.e que :

$$\deg(P_1) + \dots + \deg(P_r) = n.$$

Or on a :

$$P_1 \dots P_r = \det(XI_n - M) = \chi_M.$$

Ainsi on a la relation voulue, d'où B_f est une base de E.

Par définition des F_i, il est clair que : $E = F_1 \oplus \dots \oplus F_r$.
De plus un calcul montre que $P_j(u)_{|F_j} = 0$ donc F_j est u-stable et $u_{|F_j}$ est cyclique.
Si $Q \in K[X]$ tel que $Q(u_{|F_j}) = 0$ si et seulement si $Q(u)(v_j) = 0$.
Or par le corollaire ceci implique $P_j \mid Q \Rightarrow P_j$ est le pol minimale de $u_{|F_j}$. On a bien une décomposition de Frobenius.

Corollaire: Soit $u \in \mathcal{L}(E)$. Alors on a,

$$\mu_u = \frac{\chi_M}{\mu_{n-1}(XI_n - M)}$$

où $\mu_{n-1}(XI_n - M)$ est le pgcd unitaire des mineurs d'ordre $n-1$ de la matrice $XI_n - M$ i.e le pgcd des coefficients de ${}^t\mathrm{Com}(XI_n - M)$.

Preuve: C'est direct par la proposition d'avant. □

Conclusion:

L'algorithme de Smith dans l'anneau euclidien $\mathbb{K}[X]$, donne l'existence de deux matrices inversibles $U, V \in GL_n(\mathbb{K}[X])$ telles que:

$$U(XI_n - M)V = \begin{pmatrix} I_{n-r} & & \\ & P_1 & \\ & & \ddots \\ & & & P_r \end{pmatrix}$$

où $P_1, \dots, P_r \in \mathbb{K}[X]$ sont unitaires non constants et vérifient les relations de divisibilités $P_1 | \dots | P_r$. La matrice U (resp. V) est le produit de matrices de transvections, de transposition ou de dilatation correspondant aux opérations élémentaires effectuées sur les lignes (resp. les colonnes) de $XI_n - M$.

1) Invariants de similitude

Si l'on veut les invariants de similitudes de u, les résultats précédent montre que ce sont les $P_1, \dots, P_r$ donnés par la réduction sous forme de Smith de la matrice $XI_n - M$.
Ou si $n = 2$ ou 3 on peut les calculer en utilisant la formule:

$$P_i = \frac{\nu_{n-r+i}(XI_n - M)}{\nu_{n-r+i-1}(XI_n - M)} \quad \forall i \in [\![1, r]\!].$$

où r est le plus petit entier tel que $\nu_{n-r+1}(XI_n - M)$ est non constant.

2) Base de Frobenius:

Si on veut une base de Frobenius alors les prop précédentes nous donnent. Soient $Y_1, \dots, Y_r \in \mathbb{K}[X]^n$ les r dernières colonnes de U^{-1}.
Si on écrit $Y_j = \begin{pmatrix} R_{1j} \\ R_{nj} \end{pmatrix}$

et on pose: $v_j = \sum_{i=1}^{n} R_{ij}(u)(e_i)$.

Avec $d_j = \deg(P_j)$ alors $(v_1, u(v_1), \dots, u^{d_1-1}(v_1), \dots, v_r, u(v_r), \dots, u^{d_r-1}(v_r))$ est une base de Frobenius.

III - Application de la décomposition de Frobenius.

Proposition : Soit $M \in \mathcal{M}_n(\mathbb{K})$ alors M et ${}^tM$ sont semblables.

Preuve : Les mineurs de $XId - M$ et $XId - {}^tM = {}^t(XId - M)$ étant les mêmes, M et ${}^tM$ ont les mêmes invariants de similitude, d'où le résultat. ▨

Définition : Soit $u \in \mathcal{L}(E)$, on note :

$$\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}.$$

Le commutant de u est l'ensemble des éléments qui commutent avec u :

$$C(u) = \{v \in \mathcal{L}(E) \mid v \circ u = u \circ v\}$$

Le bi-commutant de u est l'ensemble des éléments qui commutent avec $C(u)$ i.e :

$$C_2(u) = \{v \in \mathcal{L}(E) \mid \forall u' \in C(u), v \circ u' = u' \circ v\}.$$

Rmq : Il est aisé de voir que $\mathbb{K}[u] \subset C_2(u) \subset C(u) \subset \mathcal{L}(E)$.

↳ Ls sous-algèbres.

Proposition : On a $C(u) = \mathbb{K}[u]$ ssi u est cyclique.

Preuve : $\Leftarrow$: Si u est cyclique et $v \in E$ tel que :

$$(v, u(v), \dots, u^{n-1}(v)) \text{ base de } E.$$

Soit $u' \in C(u)$ et écrivons :

$$u'(v) = a_0 v + a_1 u(v) + \dots + a_{n-1} u^{n-1}(u(v)).$$

On pose $P = \sum_{i=1}^{n-1} a_i X^i \in \mathbb{K}[X]$.

Par définition on a : $u'(v) = P(u)(v)$.

Or u' commute avec u donc commute avec u^k $\forall k \in [\![0, n-1]\!]$ ainsi :

$$u'(u^k(v)) = u^k(u'(v)) = u^k(P(u)(v))$$
$$= P(u)(u^k(v))$$

Ainsi $u' = P(u)$ sur une base donc sur E i.e $C(u) = \mathbb{K}[u]$ d'où le résultat.

$\Rightarrow$: Supposons u non cyclique, ainsi soit

$$E = F_1 \oplus \dots \oplus F_r$$

une décomposition de Frobenius. On sait que $r \geq 2$, on pose donc $u' \in \mathcal{L}(E)$ la projection sur F_1 parallèlement à $F_2 \oplus \dots \oplus F_r$.

Mq : $u' \in C(u)$

En effet si $x = x_1 + y \in E$ alors F_1 stable par u donc $u(x) = u(x_1) + u(y)$
$\in F_1 \quad \in F_2 \oplus \dots \oplus F_r$

donc $u'(x) = x_1$ donc $u'(u(x)) = u(x_1)$

donc $u(u'(x)) = u(x_1)$

Mq $u' \notin K[u]$.

On suppose le contraire donc soit $P \in K[X]$ tel que $P(u) = u'$.

Comme u' est nulle sur F_2 on a $P(u)_{|F_2} = P(u_{|F_2}) = 0$

Ainsi $P_2 | P$ car $P_2 = \pi_{u_{|F_2}}$.

De même $u' = id$ sur F_1 donc $P_1 | P - 1$.

Or

$$P_2 | P_1 | P - 1 \text{ d'où } P_2 | P - (P-1) = 1$$ donc P_2 est constant ce qui est absurde.

On montre le lemme suivant qui nous permettra de calculer le commutant et le bi-commutant.

Lemme: Soit $u \in \mathcal{L}(E)$ et $P_1, \dots, P_r$ ses invariants de similitudes. De plus soit $E = F_1 \oplus \dots \oplus F_r$ une décomposition de Frobenius de u. Enfin, pour tout $i \in [\![1, r]\!]$, soit $v_i \in F_i$ un vecteur tel que

$$d_i = \deg(P_i) \text{ et } (v_i, u(v_i), \dots, u^{d_i - 1}(v_i)) \text{ base de } F_i$$

Alors l'application :

$$\begin{aligned} \Theta : C(u) &\longrightarrow \ker(P_1(u)) \times \dots \times \ker(P_r(u)) \\ u' &\longmapsto (u'(v_1), \dots, u'(v_r)) \end{aligned}$$

est un isomorphisme de K-espaces vectoriels.

Preuve: Soit $u' \in C(u)$, pour $i \in [\![1, r]\!]$, $v_i \in F_i$ donc

$$P_i(u)(u'(v_i)) \underset{\uparrow u' \in C(u)}{=} u'(P_i(u)(v_i)) = u'(0) = 0$$

donc Θ est bien définie et est clairement linéaire.

Montrons que Θ est bijective.

Soit $u' \in C(u)$ tel que $u'(v_1) = \dots = u'(v_r) = 0$ comme u' commute avec u.

$$u'\left(\sum_{j=1}^{r}\sum_{i=0}^{d_j-1} \lambda_j^i u^i(v_j)\right) = \sum_{j=1}^{r}\sum_{i=0}^{d_j-1} \lambda_j^i\, u'(u^i(v_j)) = 0 \text{ donc } u' = 0.$$

i.e Θ injective.

Mq Θ est surjective. Soit $q_i \in \mathrm{Ker}\, P_i(u)$ et $u' \in \mathcal{L}(E)$ l'unique endo tel que.

$$u'(u^k(v_i)) = u^k(y_i)$$

Alors u' est définie sur E car sur une base.

Mq $u' \in C(u)$ i.e $u' \circ u = u \circ u'$.

Pour cela il suffit de voir que c'est vrai sur tout P_i ou sur la base.

Soit $P \in K[X]$ et $i \in [\![1, r]\!]$ on note :

$$P = Q P_i + R \text{ avec } \deg(R) \leq d_i - 1.$$

ainsi par def comme $\deg R \leq d_i - 1$ on a : $u'(R(u)(v_i)) = R(u)(y_i)$.

De plus $P_i(u)(v_i) = 0$ donc

$$P(u)(v_i) = R(u)(v_i).$$

donc $u'(P(u)(v_i)) = R(u)(y_i)$.

Or $y_i \in \mathrm{Ker}(P_i(u))$ donc $P(u)(y_i) = R(u)(y_i)$ d'où :

$$u'(P(u)(v_i)) = P(u)(y_i)$$

Ainsi pour $i \in [\![1, r]\!]$ et $k \in [\![0, d_i - 1]\!]$ on a :

$$(u' \circ u)(u^k(v_i)) = u'(u^{k+1}(v_i)) = u^{k+1}(y_i)$$

D'autre part,

$$(u \circ u')(u^k(v_i)) = u(u^k(y_i)) = u^{k+1}(y_i).$$

Ainsi $u \circ u'$ et $u' \circ u$ coïncident sur une base donc sont égaux.

Théorème : Pour tout $u \in \mathcal{L}(E)$, le bicommutant de u est $K[u]$ i.e :

$$C_2(u) = K[u]$$

Preuve : Soit $E = F_1 \oplus \dots \oplus F_r$ une décomposition de Frobenius.
Pour tout $i \in [\![1, r]\!]$, soit π_i le projecteur sur F_i parallèlement à $\bigoplus_{j \neq i} F_j$.

Soit $\varphi \in C(u)$. Comme F_i et $\bigoplus_{j \neq i} F_j$ sont stables par u, $\pi_i \in C(u)$ donc φ commute avec π_i $(\forall i \in [\![1, r]\!])$.
En particulier φ stabilise F_i et φ_{F_i} commute avec $u_{|F_i}$. Or $u_{|F_i}$ est cyclique donc par la prop il existe $Q_i \in K[X]$ tel que :

$$\varphi_{F_i} = Q_i(u_{F_i}) = Q_i(u)_{|F_i}.$$

Pour tout $j \in [\![1, r]\!]$, soit $v_j \in F_j$ un vecteur $u_{|F_i}$-cyclique. Puisque que l'on a $P_1 = \pi_u$, $\ker(P_1(u)) = E$.
D'après le lemme il existe $u_j' \in C(u)$ tel que :

$$u_j'(v_r) = 0, \dots, u_j'(v_2) = 0, u_j'(v_1) = v_j.$$

On a alors

$$(\varphi \circ u_j')(v_1) = \varphi(v_j)$$

et $(\varphi \circ u_j')(v_1) = u_j'(\varphi(v_1))$
$= u_j'(\varphi_{|F_1}(v_1))$
$= u_j'(Q_1(u)(v_1))$
$= Q_1(u)(u_j'(v_1))$
$= Q_1(u)(v_j)$

Ce qui donne :

$$\varphi(v_j) = Q_1(u)(v_j)$$

or φ et u commute donc l'égalité reste vrai sur la base de E i.e $\varphi = Q_1(u) \Rightarrow C(u) \subset K[u]$ ☒

Il nous reste la dimension de $C(u)$.

Théorème : Soient $d_1, \dots, d_r$ les degrés respectifs des invariants de similitude de u. Alors on a

$$\dim_K(C(u)) = \sum_{k=1}^{r} (2k - 1) d_k.$$

En particulier $\dim(C(u))$ et $\dim(\mathcal{L}(E))$ ont même parité.

Preuve : D'après le lemme on sait que :

$$\dim(C(u)) = \sum_{i=1}^{r} \dim(\operatorname{Ker}(P_i(u)))$$

Soit $x \in E$, on peut écrire :

$$x = \sum_{j=1}^{r} Q_j(u)(v_j) \quad \text{avec } \deg(Q_j) < d_j - 1$$

De plus cette écriture est unique.

Alors $x \in \operatorname{Ker}(P_i(u))$ ssi :

$$\sum_{j=1}^{r} (P_i Q_j)(u)(v_j) = 0$$

Or d'après un corollaire de la partie II on a : $P_j \mid P_i Q_j \quad \forall j \in [\![1, r]\!]$

Si $j \geq i$ alors $P_j \mid P_i$ donc $P_j \mid P_i Q_j$ pour tout Q_j tq $\deg(Q_j) < d_j$

Si $j < i$ alors l'ensemble des Q_j vérifient $P_j \mid P_i Q_j$ et $\deg Q_j < d_j$ est exactement les pol de la forme :

$$\frac{P_j}{P_i} R_j \text{ et } \deg(R_j) < d_i \quad (\text{car } P_i \mid P_j)$$

On en déduit que :

$$\dim(\operatorname{Ker} P_i(u)) = \sum_{j=i}^{r} d_j + \sum_{j=1}^{i-1} d_i = \sum_{j=i}^{r} d_j + (i-1)d_i$$

i \ j	1	2	3
1	1	2	3
2	2	3	
3	3		

On a ainsi :

$$\dim(C(u)) = \sum_{i=1}^{r} (i-1)d_i + \sum_{i=1}^{r} \sum_{j=i}^{r} d_j$$

$$= \sum_{i=1}^{r} (i-1)d_i + \sum_{j=1}^{r} \sum_{i=1}^{j} d_j$$

$$= \sum_{j=1}^{r} \left((j-1)d_j + j d_j \right)$$

$$= \sum_{j=1}^{r} (2j-1)d_j$$

En particulier on a :

$$\dim\left(\mathcal{L}(\ell)\right) - \dim\left(C(u)\right) = n^2 - \sum_{h=1}^{r} (2h-1)d_h$$

$$= n^2 - \sum_{h=1}^{r} 2hd_h + \sum_{h=1}^{r} d_h$$

$$= \ell\left(\frac{n(n+1)}{\ell} - \sum_{h=1}^{r} h d_h\right)$$