Réduction des endomorphismes

reduction-des-endomorphismes-2020-2021.tex

08/02/2021

Sommaire

Chapitre 0

Introduction.

Notation. On fixe les notations suivantes pour l'ensemble du cours.

– Si S est un ensemble fini, $|S|$ désigne son cardinal.
– Si $\Bbbk$ est un corps commutatif et V_1 et V_2 deux $\Bbbk$-espaces vectoriels, on note $\mathrm{Hom}_{\Bbbk}(V_1, V_2)$ le $\Bbbk$-espace vectoriel des applications $\Bbbk$-linéaires de V_1 dans V_2.
– Si E et F sont des ensembles, on note F^E l'ensemble des applications de E vers F.

– On note $\mathbb{N}$ l'ensemble de tous les entiers positifs ou nuls et on pose $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Chapitre 1

Polynômes d'endomorphismes, polynôme minimal, lemme des noyaux.

Dans tout ce chapitre, $\Bbbk$ désigne un corps commutatif.

A partir de la section 2, et jusqu'à la fin du Chapitre, E désigne un espace vectoriel sur $\Bbbk$ et f un endomorphisme de E. On suppose, en outre, que E est non nul.

1 *Rappels et compléments de structure :* Algèbre sur un corps.

Cette section rappelle la notion d'algèbre sur un corps. On suppose connue la notion d'anneau et celle d'espace vectoriel sur un corps.

Définition 1.1 – *Une algèbre sur $\Bbbk$ est un quadruplet $(A, +, \times, .)$ où A est un ensemble, $+ : A \times A \longrightarrow A$ et $\times : A \times A \longrightarrow A$ des l.c.i. de A et $. : \Bbbk \times A \longrightarrow A$ une l.c.e. à scalaires dans $\Bbbk$ tel que :*
(i) $(A, +, \times)$ soit un anneau (on note 0_A le neutre du groupe $(A, +)$ et 1_A celui de l'anneau $(A, +, \times)$) ;
(ii) $(A, +, .)$ soit un espace vectoriel sur $\Bbbk$;
(iii) pour tout $\lambda \in \Bbbk$ et tous $a, b \in A$, $\lambda.(a \times b) = (\lambda.a) \times b = a \times (\lambda.b)$.
L'algèbre $(A, +, \times, .)$ est dite commutative lorsque l'anneau sous-jacent $(A, +, \times)$ l'est.

Définition 1.2 – *Soit $(A, +, \times, .)$ une algèbre sur $\Bbbk$. Une sous-algèbre de A est un sous-ensemble de A qui est un sous-anneau de $(A, +, \times)$ et un sous-espace vectoriel de $(A, +, .)$.*

Remarque 1.3 – Les points suivants résultent facilement de la définition d'algèbre. Leur démonstration est laissée en exercice.
(i) Soit A une algèbre non nulle sur $\Bbbk$. L'application

$$\begin{array}{ccc} \Bbbk & \longrightarrow & A \\ \lambda & \mapsto & \lambda.1_A \end{array}$$

est un morphisme injectif d'anneaux dont l'image est dans le centre de A.
(ii) Soit A une algèbre sur $\Bbbk$. Tout idéal de A est un sous-espace vectoriel de A.
(iii) Soient $(A, +, \times, .)$ une algèbre sur $\Bbbk$ et B une sous-algèbre de A. L'ensemble B muni de la restriction à B des l.c.i. et l.c.e. qui définissent l'algèbre A est une algèbre sur $\Bbbk$.

Exemple 1.4 – Soit E un espace vectoriel sur $\Bbbk$. L'ensemble $\mathrm{End}_{\Bbbk}(E)$ des endomorphismes d'espace vectoriel de E est une algèbre sur $\Bbbk$ pour les opérations usuelles d'addition, de composition et de multiplication par un scalaire.

Exemple 1.5 – *Soit $n \in \mathbb{N}^*$. L'ensemble $M_n(\Bbbk)$ des matrices à n lignes et n colonnes à coefficients dans $\Bbbk$ est une algèbre sur $\Bbbk$ pour les lois usuelles.*

Exemple 1.6 – L'ensemble $\Bbbk[X]$ des polynômes en une indéterminée X et à coefficients dans $\Bbbk$ est une algèbre sur $\Bbbk$ pour les lois usuelles.

Définition 1.7 – *Soient A et B deux algèbres.*
1. Un morphisme d'algèbres de A vers B est une application $f : A \longrightarrow B$ qui est un morphisme d'anneaux et un morphisme d'espaces vectoriels.
2. Un isomorphisme d'algèbres de A vers B est un morphisme d'algèbres qui est bijectif.

Exemple 1.8 – Soit E une espace vectoriel sur $\Bbbk$ de dimension finie égale à $n \in \mathbb{N}^*$. Pour toute base $\mathcal{B}$ du $\Bbbk$-espace vectoriel E, l'application

$$\begin{array}{cccc} \mathrm{Mat}_{\mathcal{B}} & : & \mathrm{End}_{\Bbbk}(E) & \longrightarrow & \mathrm{Mat}_n(\Bbbk) \\ & & v & \mapsto & \mathrm{Mat}_{\mathcal{B}}(v) \end{array},$$

qui à tout endomorphisme de E associe sa matrice relative à $\mathcal{B}$ est un isomorphisme de $\Bbbk$-algèbres.

Proposition 1.9 – *Soient A et B des algèbres sur $\Bbbk$ et $f : A \longrightarrow B$ un morphisme d'algèbres de A vers B. Alors,*
1. le noyau de f est un idéal de A ;
2. l'image de f est une sous-algèbre de B.

Démonstration. Exercice (facile). ∎

Proposition 1.10 – *Soient A une $\Bbbk$-algèbre et a un élément de A. Il existe un morphisme d'algèbres de $\Bbbk[X]$ vers A, et un seul, qui envoie X sur a.*

Démonstration. Exercice (facile). ∎

Définition 1.11 – *Soient A une $\Bbbk$-algèbre et a un élément de A. L'unique morphisme d'algèbre de $\Bbbk[X]$ vers A qui envoie X sur a est appelé* évaluation en a *et est noté* ev_a.

Exemple 1.12 – Soit E un espace vectoriel sur $\Bbbk$. Pour tout endomorphisme f de E, on peut considérer le morphisme d'évaluation en f. C'est l'application

$$\begin{array}{cccc} \mathrm{ev}_f & : & \Bbbk[X] & \longrightarrow & \mathrm{End}_{\Bbbk}(E) \\ & & \sum_{0\leq i\leq d} \lambda_i X^i & \mapsto & \sum_{0\leq i\leq d} \lambda_i f^i \end{array}.$$

1. Les éléments de l'image de ev_f sont souvent appelés *polynômes en l'endomorphisme f*. Le sous-ensemble qu'ils forment est une sous-algèbre commutative de $\mathrm{End}_{\Bbbk}(V)$. Si $P \in \Bbbk[X]$, on pose

$$P(f) = \mathrm{ev}_f(P).$$

2. Les éléments du noyau de ev_f sont appelés *polynômes annulateurs de l'endomorphisme f*. Le sous-ensemble qu'ils forment est un idéal de $\Bbbk[X]$.
3. Si E est de dimension finie, $\mathrm{End}_{\Bbbk}(E)$ l'est aussi (cf. Exemple 1.8). L'application linéaire ev_f ne peut donc pas être injective. Il s'ensuit que ev_f a un noyau qui n'est pas réduit à $\{0\}$.

Proposition 1.13 – *Soit A une algèbre sur $\Bbbk$ et soit I un idéal de A. Il existe une application*

$$\Bbbk \times A/I \longrightarrow A/I$$

telle que, pour tout $\lambda \in \Bbbk$ et tout $a \in A$, l'image de $(\lambda, a + I)$ soit $\lambda.a + I$. De plus, $(A/I, +, \times, .)$ est une algèbre sur $\Bbbk$, où $+$ et $\times$ sont les l.c.i. naturelles de l'anneau quotient A/I et . la l.c.e. déterminée par l'application ci-dessus. De plus :
1. la projection canonique $A \longrightarrow A/I$ est un morphisme d'algèbres sur $\Bbbk$;

2. si B est une algèbre sur $\Bbbk$, $f : A \longrightarrow B$ un morphisme d'algèbres et I un idéal de A dans le noyau de f, alors l'unique morphisme d'anneaux g qui rend le diagramme

$$\begin{tikzcd} A \arrow[rr, "\pi"] \arrow[drr, "f"'] & & A/I \arrow[d, "g"] \\ & & B \end{tikzcd}$$

commutatif est un morphisme d'algèbres sur $\Bbbk$.

Démonstration. Exercice. ∎

Remarque 1.14 – Soit $(A, +, \times)$ un anneau.
1. On suppose donnée une structure d'algèbre sur $\Bbbk$ dont l'anneau sous-jacent est $(A, +, \times)$. Comme on a vu ci-dessus, cela détermine un morphisme d'anneaux $\iota_k : \Bbbk \longrightarrow A$, à valeurs dans le centre de A.
2. Supposons donné un morphisme d'anneaux $\alpha : \Bbbk \longrightarrow A$. L'application

$$\begin{array}{cccc} . \ : & \Bbbk \times A & \longrightarrow & A \\ & (\lambda, a) & \mapsto & \alpha(\lambda)a \end{array}$$

est une loi de composition interne et $(A, +, \times, .)$ est une algèbre dont l'anneau sous-jacent est $(A, +, \times)$.
3. Les deux constructions ci-dessous sont réciproques l'une de l'autre. Ainsi, la donnée d'une structure d'algèbre sur $\Bbbk$ sur un anneau $(A, +, \times)$ est-elle équivalente à celle d'un morphisme d'anneaux $\Bbbk \longrightarrow A$ à valeur dans le centre de $(A, +, \times)$.
4. Soit $(A, +, \times, .)$ une algèbre sur le corps $\Bbbk$ et I un idéal de A. On considère l'anneau quotient A/I et le morphisme d'anneaux $\Bbbk \longrightarrow A \longrightarrow A/I$ où la première flèche est celle définie à la Remarque 1.3 et la seconde la projection canonique d'un anneau sur son anneau quotient par un idéal. Si l'on applique la construction décrite au point 2 ci-dessus, on retrouve la structure d'algèbre sur A/I définie au premier point de la Proposition 1.13.

2 Polynôme minimal d'un endomorphisme.

A partir de maintenant, et jusqu'à la fin du Chapitre, E désigne un espace vectoriel sur $\Bbbk$ et f un endomorphisme de E. On suppose, en outre, que E est non nul.

On a vu à la section 1, Exemple 1.12, qu'on peut attacher à la donnée de E et de f un morphisme d'algèbres comme suit :

$$\begin{array}{cccc} \mathrm{ev}_f \ : & \Bbbk[X] & \longrightarrow & \mathrm{End}_{\Bbbk}(E) \\ & \sum_{0 \leq i \leq d} \lambda_i X^i & \mapsto & \sum_{0 \leq i \leq d} \lambda_i f^i \end{array}.$$

Si $P \in \Bbbk[X]$, on pose $\mathrm{ev}_f(P) = P(f)$. On notera alors qu'on a l'identité ci-dessous :

$$\forall\, P, Q \in \Bbbk[X], \quad (PQ)(f) = P(f) \circ Q(f). \tag{1.1}$$

On pose $\Bbbk[f] = \mathrm{Im}(\mathrm{ev}_f)$; c'est une sous-algèbre commutative de $\mathrm{End}_{\Bbbk}(E)$. Les éléments de $\Bbbk[f]$ sont appelés les polynômes de l'endomorphisme f et on a :

$$\Bbbk[f] = \{P(f),\, P \in \Bbbk[X]\}.$$

Les éléments du noyau de ev_f sont appelés les polynômes annulateurs de f. Il est clair que tout polynôme annulateur non nul de f est de degré au moins égal à 1. On a un isomorphisme d'algèbres sur $\Bbbk$ comme suit :

$$\Bbbk[X]/\ker(\mathrm{ev}_f) \cong \Bbbk[f].$$

Remarque 2.1 – **Polynômes d'endomorphismes et restrictions.** On suppose que F est un sous-espace vectoriel de E stable par f et on note $f_{|F}$ l'endomorphisme de F induit par f.
1. Il est clair que, pour tout $P \in \mathbb{k}[X]$, $P(f)$ laisse F stable et que, si $P(f)_{|F}$ désigne l'endomorphisme induit sur F par $P(f)$, on a :

$$P(f_{|F}) = P(f)_{|F}.$$

2. D'après le premier point, le morphisme d'évaluation en $f_{|F}$ est le suivant :

$$\begin{array}{rccc} \mathrm{ev}_{f_{|F}} & : & \mathbb{k}[X] & \longrightarrow & \mathrm{End}_{\mathbb{k}}(F) \\ & & P & \mapsto & P(f)_{|F} \end{array}.$$

Proposition 2.2 – *On suppose que E est de dimension finie. Alors, il existe un unique polynôme unitaire μ dans $\mathbb{k}[X]$ tel que l'on ait :*

$$\ker(\mathrm{ev}_f) = \langle \mu \rangle.$$

Démonstration. Comme E est de dimension finie, ev_f ne peut pas être injective (cf. Exemple 1.12, Point 3). Ainsi, $\ker(\mathrm{ev}_f)$ est un idéal non nul de l'anneau $\mathbb{k}[X]$. Mais, $\mathbb{k}[X]$ est un anneau principal. Il existe donc une unique polynôme unitaire μ de $\mathbb{k}[X]$ qui engendre l'idéal $\ker(\mathrm{ev}_f)$. ∎

Définition 2.3 – *On suppose que E est de dimension finie. L'unique générateur unitaire de l'idéal* $\ker(\mathrm{ev}_f)$ *(cf. Proposition 2.2) est appelé le polynôme minimal de l'endomorphisme f et est noté μ_f.*

Remarque 2.4 – On suppose que E est de dimension finie. Il est important de remarquer que le polynôme minimal d'un endomorphisme sur un espace vectoriel non nul n'est jamais un polynôme constant. En effet, si $\lambda \in \mathbb{k}$, le polynôme constant $P = \lambda$ a pour image par ev_f l'homothétie de rapport λ qui, puisque E est non nul, n'est pas l'endomorphisme nul.

Remarque 2.5 – On suppose que E est de dimension finie. Si F est un sous-espace vectoriel de E stable par f et si l'on note g l'endomorphisme de F induit par f, on a :

$$\mu_g | \mu_f.$$

Il est clair en effet que μ_f est annulateur de g.

Exemple 2.6 – On suppose que E est de dimension finie.
1. Le polynôme minimal de f est de degré 1 si et seulement si f est une homothétie. De plus, si f est l'homothétie de rapport $\lambda \in \mathbb{k}$, son polynôme minimal est $X - \lambda$.
2. Soient F et G deux sous-espaces vectoriels supplémentaires de E et soit $\lambda \in \mathbb{k}$. On rappelle que l'*affinité vectorielle* de base F, de direction G et de rapport λ est l'endomorphisme d de E tel que, pour tout $x \in F$ et $y \in G$,

$$d(x + y) = x + \lambda y.$$

(On note que, si $\lambda = 1$, d n'est autre que l'identité de E, que si $\lambda = 0$, d est la projection sur F, parallèlement à G et que si $\lambda = -1$, d est la symétrie par rapport à F parallèlement à G.) Si F ou G est le sous-espace nul, ou si $\lambda = 1$, d est une homothétie. Dans la suite, on exclut ce cas, ce qui entraine en particulier que d n'est pas une homothétie.

On vérifie facilement que $(X - 1)(X - \lambda)$ est un polynôme annulateur de d et qu'aucun polynôme de degré 1 n'annule f. Il s'ensuit que le polynôme minimal de d est $(X - 1)(X - \lambda)$.
3. On rappelle qu'un endomorphisme g de E est dit nilpotent s'il existe un entier naturel i non nul tel que $g^i = 0$. De plus, pour un tel endomorphisme, l'ensemble $\{i \in \mathbb{N}^* | g^i = 0\}$ est non vide et admet donc un plus petit élément que l'on appelle l'indice de nilpotence de g. Un endomorphisme g de E est nilpotent d'indice d si et seulement si son polynôme minimal est X^d.

Proposition 2.7 – *On suppose que E est de dimension finie et on note d le degré du polynôme minimal de l'endomorphisme f. Alors, la famille $(f^j)_{0 \leq j \leq d-1}$ est une base du $\mathbb{k}$-espace vectoriel $\mathbb{k}[f]$.*

Démonstration. On rappelle que $d \in \mathbb{N}^*$ (cf. Remarque 2.4). Par définition, $\Bbbk[f]$ est l'image de l'application linéaire $\mathrm{ev}_f : \Bbbk[X] \longrightarrow \mathrm{End}_{\Bbbk}(E)$. Comme la famille $(X^i,\, i \in \mathbb{N})$ est une base de $\Bbbk[X]$, la famille $(f^i,\, i \in \mathbb{N})$ est donc une famille génératrice de $\Bbbk[f]$. Soient $\lambda_0, \dots, \lambda_{d-1} \in \Bbbk$ tels que $\mu = X^d + \sum_{0 \le i \le d-1} \lambda_i X^i$.
1. Pour $k \in \mathbb{N}$, on pose

$$\mathcal{F}_k = \mathrm{Vect}\{f^i,\, 0 \le i \le k\}.$$

Ainsi, on a une suite croissante de sous-espaces vectoriels de $\Bbbk[f]$:

$$\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \ldots \subseteq \mathcal{F}_{d-1} \subseteq \mathcal{F}_d \subseteq \ldots \subseteq \Bbbk[f].$$

On va montrer, par récurrence sur k, que pour tout $k \ge d$, $\mathcal{F}_k = \mathcal{F}_{d-1}$. Comme μ_f est annulateur de f, $f^d = -\sum_{0 \le i \le d-1} \lambda_i f^i$. Il s'ensuit que $f^d \in \mathcal{F}_{d-1}$ et donc que $\mathcal{F}_d = \mathcal{F}_{d-1}$.

Supposons à présent que $k \ge d$ est un entier tel que $\mathcal{F}_k = \mathcal{F}_{d-1}$. Alors, pour tout entier i tel que $i \le k$, on a $f^i \in \mathcal{F}_{d-1}$. En outre, en composant la relation $f^d = -\sum_{0 \le i \le d-1} \lambda_i f^i$ par f^{k+1-d}, on obtient que $f^{k+1} = -\sum_{0 \le i \le d-1} \lambda_i f^{i+k+1-d} \in \mathcal{F}_k = \mathcal{F}_{d-1}$. Ce qui démontre que $\mathcal{F}_{k+1} = \mathcal{F}_{d-1}$ et termine la récurrence.

A ce stade, on a donc démontré que

$$\Bbbk[f] = \mathrm{Vect}(f^i,\, 0 \le i \le d-1).$$

2. On montre maintenant que la famille $(f^i,\, 0 \le i \le d-1)$ de $\Bbbk[f]$ est libre. Supposons, au contraire, qu'elle soit liée. Alors, il existe des scalaires $\lambda_0, \dots, \lambda_{d-1} \in \Bbbk$, non tous nuls, tels que

$$\sum_{0 \le i \le d-1} \lambda_i f^i = 0,$$

ce qui revient à dire que le polynôme non nul $\sum_{0 \le i \le d-1} \lambda_i X^i$ est annulateur de f. Mais ce polynôme est de degré strictement plus petit que le degré de μ_f. Il ne peut donc pas être multiple de μ_f ; c'est une contradiction.

Ainsi, on a démontré que la famille $(f^i,\, 0 \le i \le d-1)$ de $\Bbbk[f]$ est libre et génératrice de $\Bbbk[f]$. ■

Proposition 2.8 – *On suppose que E est de dimension finie et on note μ le polynôme minimal de l'endomorphisme f.*
(i) L'endomorphisme f est inversible si et seulement si $\mu(0) \neq 0$.
(ii) Si f est inversible, alors $f^{-1} \in \Bbbk[f]$.

Démonstration. On note d le degré du polynôme minimal de f et on pose $\mu = \sum_{0 \le i \le d} a_i X^i$, où, pour $0 \le i \le d$, $a_i \in \Bbbk$. (En particulier, $a_0 = \mu(0)$ et $a_d = 1$.) On a donc la relation

$$\sum_{0 \le i \le d} a_i f^i = \mu(f) = 0. \tag{1.2}$$

1. Supposons que $a_0 = 0$. On peut mettre f en facteur dans la relation (1.2) et on obtient ainsi :

$$f \circ \left(\sum_{1 \le i \le d} a_i f^{i-1} \right) = 0.$$

Mais, par définition du polynôme minimal, le polynôme $\sum_{1 \le i \le d} a_i X^{i-1}$ ne peut annuler f puisqu'il est de degré au plus égal à $d-1$. Il s'ensuit l'existence de $x \in E$ tel que $\left(\sum_{1 \le i \le d} a_i f^{i-1} \right)(x) \neq 0$, ce dont il découle que le noyau de f n'est pas réduit à 0. Ainsi f n'est pas inversible. Par suite, si f est inversible, alors $\mu(0) \neq 0$.
2. Supposons que $a_0 \neq 0$. En multipliant (1.2) par a_0^{-1} et en isolant id_E, on obtient

$$\mathrm{id}_E = f \circ \left(\sum_{1 \le i \le d} (-a_0)^{-1} a_i f^{i-1} \right),$$

qui assure que f est inversible et que $f^{-1} \in \Bbbk[f]$. ■

3 Sous-espaces stables remarquables ; lemme des noyaux.

Si $P \in \Bbbk[X]$, alors $P(f)$ est un endomorphisme de E qui commute avec f. Il s'ensuit immédiatement que son noyau, $\ker(P(f))$, est un sous-espace vectoriel de E stable par f. Dans cette section, on s'attache à l'étude des sous-espaces vectoriels de cette forme. Il s'avèrera, en effet, que leur rôle est crucial dans la réduction de l'endomorphisme f.

Le résultat clé est le *lemme de noyaux*. Il résulte des propriétés arithmétiques de $\Bbbk[X]$ et permet de démontrer que, lorsque E est de dimension finie, il se décompose en somme directe de tels noyaux qui, par ailleurs, sont en nombre fini.

Lemme 3.1 – *Soient $P, Q \in \Bbbk[X]$.*
1. Si D est un p.g.c.d. de P et Q, alors $\ker(P(f)) \cap \ker(Q(f)) = \ker(D(f))$.
2. Si P et Q sont premiers entre eux, alors

$$\ker((PQ)(f)) = \ker(P(f)) \oplus \ker(Q(f)).$$

Démonstration. 1. Les polynômes P et Q sont des multiples de D. L'inclusion $\supseteq$ découle donc facilement de l'identité (1.1). D'autre part, par définition d'un p.g.c.d., il existe $U, V \in \Bbbk[X]$ tels que $D = UP + VQ$. On a alors $D(f) = U(f) \circ P(f) + V(f) \circ Q(f)$. L'inclusion $\subseteq$ s'ensuit facilement.
2. Puisque P et Q sont premiers entre eux, 1 est un p.g.c.d. de P et Q. Le premier point montre alors que $\ker(P(f)) \cap \ker(Q(f)) = \ker(\mathrm{id}_E) = (0)$, c'est-à-dire que la somme de $\ker(P(f))$ et $\ker(Q(f))$ est directe. En utilisant (1.1), il est clair, par ailleurs, que $\ker(P(f)) \subseteq \ker((PQ)(f))$ et $\ker(Q(f)) \subseteq \ker((PQ)(f))$. Donc $\ker(P(f)) \oplus \ker(Q(f)) \subseteq \ker((PQ)(f))$. Soient en outre $U, V \in \Bbbk[X]$ tels que $UP + VQ = 1$. On a l'identité $\mathrm{id}_E = U(f) \circ P(f) + V(f) \circ Q(f)$. Soit alors $x \in \ker((PQ)(f))$. La précédente identité assure que

$$x = U(f)(P(f)(x)) + V(f)(Q(f)(x)).$$

Mais, comme $x \in \ker((PQ)(f))$, $U(f)(P(f)(x)) \in \ker(Q(f))$ et $V(f)(Q(f)(x)) \in \ker(P(f))$. Il s'ensuit que $\ker(P(f)) \oplus \ker(Q(f)) \supseteq \ker((PQ)(f))$. ∎

Proposition 3.2 – ***Lemme des noyaux.***
Soient $N \in \mathbb{N}^*$, $P_1, \ldots, P_N$ des éléments de $\Bbbk[X]$ deux à deux premiers entre eux et $P = \prod_{1 \le k \le N} P_k$.
1. On a

$$\ker(P(f)) = \bigoplus_{1 \le k \le N} \ker(P_k(f)).$$

2. On suppose que $P(f) = 0$. Alors, on a $E = \bigoplus_{1 \le k \le N} \ker(P_k(f))$ et, pour tout $1 \le k \le N$, la projection sur $\ker(P_k(f))$ parallèlement à $\bigoplus_{1 \le i \le N, i \ne k} \ker(P_i(f))$ est un élément de $\Bbbk[f]$.

Démonstration. 1. On procède par récurrence sur N. Le cas $N = 1$ est trivial. Supposons le résultat vrai pour une certain entier N, $N \in \mathbb{N}^*$. Soient $P_1, \ldots, P_{N+1}$ des éléments de $\Bbbk[X]$ deux à deux premiers entre eux et $P = \prod_{1 \le k \le N} P_k$. Comme les P_i sont deux à deux premiers entre eux, P et P_{N+1} le sont aussi. Le Lemme 3.1 assure donc que

$$\ker((PP_{N+1})(f)) = \ker(P(f)) \bigoplus \ker(P_{N+1}(f)).$$

L'hypothèse de récurrence conduit donc à l'identité

$$\ker((PP_{N+1})(f)) = \left(\bigoplus_{1 \le k \le N} \ker(P_k(f)) \right) \bigoplus \ker(P_{N+1}(f)).$$

L'assertion est donc vraie au rang $N + 1$. Le point 1 est démontré.
2. Notons que, puisqu'on suppose que $P(f) = 0$, d'après le point 1, on a bien

$$E = \ker(P(f)) = \bigoplus_{1 \le k \le N} \ker(P_k(f)).$$

Le résultat est trivial pour $N = 1$ puisqu'alors la projection en question est l'identité. On suppose désormais que $N \geq 2$. On pose $Q = \prod_{1\leq i\leq N,\, i\neq k} P_i$. Comme on suppose que $P(f) = 0$, d'après le premier point, on a
$$E = \ker(P_k(f)) \bigoplus \ker(Q(f)) \tag{1.3}$$
et on s'intéresse au projecteur sur $\ker(P_k(f))$ parallèlement à $\ker(Q(f))$. Notons p_k ce projecteur. La primalité relative de P_k et Q assure qu'il existe $U, V \in \Bbbk[X]$ tels que $UP_k + VQ = 1$.

Pour tout $x \in E$, on a alors
$$x = ((UP_k + VQ)(f))(x) = ((UP_k)(f))(x) + ((VQ)(f))(x),$$
avec $((UP_k)(f))(x) \in \ker(Q(f))$ et $((VQ)(f))(x) \in \ker(P_k(f))$. Ainsi, par définition de p_k, $p_k(x) = ((VQ)(f))(x)$.

On a donc montré que $p_k = (VQ)(f)$. Le point 2 est établi. ■

Corollaire 3.3 – *On considère un polynôme P annulateur de f et non nul. Soit*
$$P = \prod_{1\leq k\leq N} P_k^{\alpha_k}$$
la décomposition de P en produit d'irréductibles, où $N \in \mathbb{N}^*$, les $P_1, \ldots, P_N$ sont des polynômes irréductibles deux à deux distincts et $\alpha_1, \ldots, \alpha_N$ des entiers naturels non nuls.
1. On a
$$E = \bigoplus_{1\leq k\leq N} \ker(P_k^{\alpha_k}(f)).$$
2. Soit F un sous-espace vectoriel de E stable par f. On a
$$F = \bigoplus_{1\leq k\leq N} \left(F \cap \ker(P_k^{\alpha_k}(f))\right).$$

Démonstration. Le premier point est une conséquence immédiate du premier point du Lemme des noyaux, puisque $\ker(P(f)) = E$. Démontrons le second point. Il est clair que les sous-espaces vectoriels $F \cap \ker(P_k^{\alpha_k}(f))$, $1 \leq k \leq N$, sont en somme directe puisque les sous-espaces $\ker(P_k^{\alpha_k}(f))$, $1 \leq k \leq N$, le sont d'après le premier point. On a donc
$$F \supseteq \bigoplus_{1\leq k\leq N} (F \cap \ker(P_k^{\alpha_k}(f)))$$
et il reste à démontrer l'égalité de ces sous-espaces. Soit $x \in F$. D'après le premier point, il existe $x_k \in \ker(P_k^{\alpha_k}(f))$, $1 \leq k \leq N$, tels que $x = x_1 + \ldots + x_N$. De plus, pour $1 \leq k \leq N$, x_k est le projeté de x sur $\ker(P_k^{\alpha_k}(f))$ parallèlement à $\bigoplus_{j\neq k} \ker(P_j^{\alpha_j}(f))$. Mais, d'après le second point du Lemme des noyaux, la projection sur $\ker(P_k^{\alpha_k}(f))$ parallèlement à $\bigoplus_{j\neq k} \ker(P_j^{\alpha_j}(f))$ est un élément de $\Bbbk[f]$. Il existe donc $Q \in \Bbbk[X]$ tel que cette projection soit $Q(f)$ et par conséquent tel que $x_k = (Q(f))(x)$. La stabilité de F par f assure donc que $x_k \in F$. ■

Remarque 3.4 – On reprend les notations du Corollaire 3.3. Pour tout $1 \leq k \leq N$, le sous-espace vectoriel $\ker(P_k^{\alpha_k}(f))$ est une sous-espace de E stable par F. Le premier point du Corollaire 3.3 associe donc, à tout polynôme non nul annulateur de f une décomposition de E en sous-espaces stables par f.
Si E est de dimension finie, on sait qu'il existe des polynômes non nuls annulateurs de f, par exemple le polynôme minimal de f. Ce qui précède fournit donc effectivement des décomposition de E en sous-espaces stables par f.

Remarque 3.5 – ***Sur les noyaux d'éléments de $\Bbbk[f]$.***
1. Soit P dans $\Bbbk[X]$. On a déjà remarqué que le sous-espace vectoriel $\ker(P(f))$ de E est stable par f. Les sous-espaces de cette forme auront une importance centrale dans la réduction de l'endomorphisme f.
2. On suppose que μ est un polynôme annulateur de f. Soit P dans $\Bbbk[X]$. Si l'on applique le Lemme 3.1 aux polynômes μ et P, on obtient que $\ker(P(f)) = \ker(D(f))$, où D est un diviseur de μ. Il s'ensuit

que l'ensemble des sous-espaces de E de la forme $\ker(P(f))$ avec $P \in \Bbbk[X]$ est fini dès que f admet un polynôme annulateur non nul.
3. On suppose que E est de dimension finie et on note μ_f le polynôme minimal de f. Alors,

$$\{\ker(P(f)),\ P \in \Bbbk[X]\} = \{\ker(P(f)),\ P \in \Bbbk[X],\ P|\mu_f\}.$$

En particulier, $\{\ker(P(f)),\ P \in \Bbbk[X]\}$ est de cardinal fini.

Exemple 3.6 – Soient F et G deux sous-espaces vectoriels non nuls de E supplémentaires et soit p la projection sur F, parallèlement à G. (Voir l'exemple 2.6.) Puisque le polynôme minimal de p est $X(X-1)$, d'après la Remarque 3.5, l'ensemble $\{\ker(P(f)),\ P \in \Bbbk[X]\}$ est constitué des sous-espaces E, F, G et $\{0\}$.

Attention cependant : il existe d'autres sous-espaces de E stables par p. C'est le cas de tout sous-espace obtenu comme somme (directe) d'un sous-espace de F et d'un sous-espace de G. Le second point du corollaire 3.3 montre qu'en fait un sous-espace de E est stable par p si et seulement si il est somme (directe) d'un sous-espace de F et d'un sous-espace de G.

Remarque 3.7 – ***Sur les noyaux d'éléments de*** $\Bbbk[f]$ ***avec*** f ***nilpotent.*** On suppose que f est un endomorphisme nilpotent de E dont on note d l'indice de nilpotence. La Remarque 3.5 donne

$$\{\ker(P(f)),\ P \in \Bbbk[X]\} = \{\ker\left(f^i\right),\ 0 \leq i \leq d\}.$$

De plus, le cardinal de l'ensemble ci-dessus est $d+1$ (cf. Exercice 4.4).

On peut démontrer directement (cf. Exercice 4.5) que, si E est de dimension finie et que $d = \dim_{\Bbbk}(E)$, les seuls sous-espaces de E stables par f sont les $\ker\left(f^i\right)$, $0 \leq i \leq d$.

Lemme 3.8 – ***Sur les suites de noyaux itérés.***
1. Soit $P \in \Bbbk[X]$.
1.1. La suite $(\ker(P^i(f)))_{i\in\mathbb{N}}$ *est une suite croissante (pour l'inclusion) de sous-espaces vectoriels de* E.
1.2. Il existe $\ell \in \mathbb{N} \cup \{\infty\}$*, unique, tel que* $\ker(P^i(f)) \subset \ker(P^j(f))$ *pour tous entiers naturels* i, j *tels que* $i < j \leq \ell$ *et* $\ker(P^\ell(f)) = \ker(P^j(f))$ *pour tous entiers naturels* j *tels que* $\ell \leq j$*. De plus, si* E *est de dimension finie,* $\ell \in \mathbb{N}$.
2. On suppose E *de dimension finie, on note* μ_f *le polynôme minimal de* f *et on écrit*

$$\mu_f = \prod_{1\leq k\leq N} P_k^{\alpha_k}$$

la décomposition de μ_f *en produit de puissances d'irréductibles, où* $N \in \mathbb{N}^*$*, les* $P_1, \ldots, P_N$ *sont des polynômes irréductibles deux à deux distincts et* $\alpha_1, \ldots, \alpha_N$ *des entiers naturels non nuls. Alors, pour tout* $1 \leq k \leq N$*, on a*

$$0 \subset \ker(P_k(f)) \subset \ldots \subset \ker(P_k^{\alpha_k-1}(f)) \subset \ker(P_k^{\alpha_k}(f))$$

(suite strictement croissante) et, pour $\beta \in \mathbb{N}$*,* $\beta \geq \alpha_k$*,* $\ker(P_k^{\alpha_k}(f)) = \ker(P_k^{\beta}(f))$.

Démonstration. 1. On ne donne qu'une esquisse de démonstration ; les détails sont laissés en exercice. (On conseille aussi au lecteur de faire le lien avec la première question de l'exercice 4.4.)
1.1. Cela découle du fait que, pour $i \in \mathbb{N}$, $P^{i+1}(f) = P(f) \circ P^i(f)$.
1.2. On peut démontrer facilement la propriété suivante : si i est un entier naturel tel que $\ker(P^i(f)) = \ker(P^{i+1}(f))$, alors $\ker(P^{i+1}(f)) = \ker(P^{i+2}(f))$. Ainsi, si deux sous-espaces consécutifs de la suite $(\ker(P^i(f)))_{i\in\mathbb{N}}$ sont égaux, la suite est stationnaire (c'est-à-dire que tous ses termes sont égaux à partir d'un certain rang). Le résultat en découle.
2. Soit $1 \leq k \leq N$. Montrons d'abord que $\ker(P_k^{\alpha_k-1}(f)) \subset \ker(P_k^{\alpha_k}(f))$. Supposons que

$$\ker(P_k^{\alpha_k-1}(f)) = \ker(P_k^{\alpha_k}(f)), \tag{1.4}$$

et posons $Q = P_k^{\alpha_k-1} \prod_{1\leq i\leq N,\, i\neq k} P_i^{\alpha_i}$. D'après le Corollaire 3.3, on a

$$E = \bigoplus_{1\leq i\leq N} \ker(P_i^{\alpha_i}(f)). \tag{1.5}$$

Il resulte alors de l'égalité (1.4) que $Q(f)=0$ et donc que μ_f divise Q. C'est une contradiction. On a donc $\ker(P_k^{\alpha_k-1}(f))\subset\ker(P_k^{\alpha_k}(f))$. Compte tenu du Point 1, on en déduit que

$$0\subset\ker(P_k(f))\subset\ldots\subset\ker(P_k^{\alpha_k-1}(f))\subset\ker(P_k^{\alpha_k}(f)).$$

Soit à présent un entier β, $\beta\geq\alpha_k$. Le polynôme $P_k^{\beta-\alpha_k}\mu_f$ annule f. D'après le Corollaire 3.3, on a donc

$$E=\left(\bigoplus_{1\leq i\leq N,i\neq k}\ker(P_i^{\alpha_i}(f))\right)\bigoplus\ker(P_k^{\beta}(f)). \tag{1.6}$$

En comparant les décompositions (1.5) et (1.6), et puisque $\ker(P_k^{\alpha_k}(f))\subseteq\ker(P_k^{\beta}(f))$, on obtient que $\ker(P_k^{\alpha_k}(f))=\ker(P_k^{\beta}(f))$. ∎

Proposition 3.9 – *On suppose que E est de dimension finie et on note μ_f le polynôme minimal de f. L'application*

$$\begin{array}{ccc}\{D\in\Bbbk[X],\ D\ \textit{unitaire},\ D|\mu_f\} & \longrightarrow & \{\ker(P(f)\},\ P\in\Bbbk[X]\}\\ D & \mapsto & \ker(D(f))\end{array}$$

est une bijection.

Démonstration. La Remarque 3.5 assure que cette application est surjective. Ecrivons

$$\mu_f=\prod_{1\leq k\leq N}P_k^{\alpha_k}$$

la décomposition de μ_f en produit d'irréductibles, où $N\in\mathbb{N}^*$, les $P_1,\ldots,P_N$ sont des polynômes irréductibles deux à deux distincts et $\alpha_1,\ldots,\alpha_N$ des entiers naturels non nuls. D'après le Corollaire 3.3, on a

$$E=\bigoplus_{1\leq k\leq N}\ker(P_k^{\alpha_k}(f)).$$

La donnée d'un diviseur unitaire D de μ_f est équivalente à celle d'un N-uplet d'entiers $(\beta_1,\ldots,\beta_N)$ tel que, pour $1\leq i\leq N$, $0\leq\beta_i\leq\alpha_i$. De plus, pour un tel diviseur, le Lemme des Noyaux assure que

$$\ker(D(f))=\bigoplus_{1\leq k\leq N}\ker(P_k^{\beta_k}(f)).$$

Il suffit alors d'appliquer le second point du Lemme 3.8 pour conclure. ∎

4 *Exercices.*

Exercice 4.1 – On considère l'espace vectoriel $E=\Bbbk[X]$ et l'endomorphisme ∂ de dérivation formelle sur E. Montrer que, si $\Bbbk$ est de caractéristique nulle, l'endomorphisme ∂ n'admet pas de polynôme annulateur différent de 0. Qu'en est-il en caractéristique strictement positive ?

Exercice 4.2 – Soit E un espace vectoriel sur $\Bbbk$, de dimension finie, et soient F,G des sous-espaces vectioriels de E tels que $E=F\oplus G$ et stables par f. On note $f_{|F}$ et $f_{|G}$ les endomorphismes de F et G respectivement induits par f sur F et G. Démontrer que μ_f est le p.p.c.m. de $\mu_{f_{|F}}$ et $\mu_{f_{|G}}$.

Exercice 4.3 – Soit E un espace vectoriel sur $\Bbbk$ et f un projecteur de E. Montrer qu'un sous-espace vectoriel de E est stable par f si et seulement si il est somme (directe) d'un sous-espace vectoriel de $\ker(f)$ et d'un sous-espace vectoriel de $\mathrm{Im}(f)$. (Voir la Remarque 3.6.)

Exercice 4.4 – **Sur les endomorphismes nilpotents.**
Soit E un espace vectoriel sur $\Bbbk$ et f un endomorphisme de E.
1. Montrer que la suite $(\ker(f^j))_{j\in\mathbb{N}}$ est une suite croissante (pour l'inclusion) de sous-espaces vectoriels

de E et que si k est un entier naturel tel que $\ker(f^k) = \ker(f^{k+1})$, alors $\ker(f^j) = \ker(f^k)$ pour tout entier j tel que $j \geq k$.
2. On suppose que la suite $(\ker(f^j))_{j\in\mathbb{N}}$ est stationnaire et on note p le plus petit entier naturel j tel que $\ker(f^j) = \ker(f^{j+1})$. Montrer que, pour $0 \leq j \leq p$, $\dim_{\mathbb{k}}(\ker(f^j) \geq j$.
3. On suppose que f est nilpotent d'indice d. Montrer qu'alors la suite $(\ker(f^j))_{j\in\mathbb{N}}$ est stationnaire et que d est le plus petit entier naturel j tel que $\ker(f^j) = \ker(f^{j+1})$.
4. On suppose que E est de dimension finie et f nilpotent. Montrer qu'il existe une base de E relativement à laquelle la matrice de f est triangulaire supérieure stricte.
5. On suppose E de dimension finie égale à $n \in \mathbb{N}^*$ et un suppose f nilpotent d'indice n. Montrer que, pour $0 \leq i \leq n$, on a $\dim_{\mathbb{k}}(\ker(f^i)) = i$.

Exercice 4.5 – **Sur les sous-espaces stables des endomorphismes nilpotents.**
On suppose que f est un endomorphisme nilpotent de E dont on note d l'indice de nilpotence. On rappelle (cf. Exercice 4.4) qu'on a alors une suite strictement croissante de sous-espace de E stables par f :

$$\{0\} \subset \ker(f) \subset \ldots \subset \ker(f^{d-1}) \subset \ker(f^d) = E. \tag{1.7}$$

On suppose que E est de dimension finie et que $d = \dim_{\mathbb{k}}(E)$. Le but de cet exercice est de montrer que les $d+1$ sous-espaces de la suite (1.7) sont les seuls sous-espaces de E stables par f.

Soit F un sous-espace de E stable par f.
1. Montrer que l'endomorphisme $f_{|F}$ de F induit par E est nilpotent d'indice majoré par d. On note k son indice de nilpotence.
2. Montrer que $F \cap \ker(f^k) = \ker(f^k_{|F}) = F$, puis que $\ker(f^k) \supseteq F$.
3. Montrer que $\dim_{\mathbb{k}}(\ker(f^k)) = k$ et que $\dim(F) = \dim(\ker(f^k_{|F}) \geq k$ (on pourra utiliser l'Exercice 4.4).
4. Conclure que $F = \ker(f^k)$.

Chapitre 2

Sous-espaces cycliques et applications.

Dans tout ce chapitre, $\Bbbk$ désigne un corps commutatif, E un espace vectoriel sur $\Bbbk$ et f un endomorphisme de E. On suppose, en outre, que E est non nul.

1 Sous-espaces cycliques ; endomorphismes cycliques.

Lemme 1.1 – *Soit $x \in E$.*
1. On considère un ensemble non vide I et $(V_i)_{i\in I}$ une famille de sous-espaces vectoriels de E contenant x et stables par f. Alors, $\cap_{i\in I} V_i$ est un sous-espace vectoriel de E contenant x et stable par f.
2. L'ensemble des sous-espaces vectoriels de E contenant x et stables par f admet un plus petit élément (pour l'inclusion).

Démonstration. Il est immédiat que l'intersection d'une famille de sous-espaces vectoriels qui contiennent x est un sous-espace vectoriel qui contient x. Il est clair aussi que l'intersection d'une famille de sous-espaces vectoriels stables par f est stable par f. Ceci démontre le premier point. On démontre maintenant le second point. On observe d'abord que E est un sous-espace vectoriel contenant x et stable par f. Par suite, la famille de tous les sous-espaces vectoriels de E contenant x et stables par f est indexée par un ensemble non vide. Le premier point s'applique donc et montre que l'intersection de tous les sous-espaces vectoriels de E, contenant x et stables par f est un sous-espace vectoriel contenant x et stable par f. Soit V cette intersection. Il est évident que V est inclus dans tout sous-espace vectoriel contenant x et stable par f. Ceci démontre le second point. ■

Définition 1.2 – *Soit $x \in E$. Le plus petit sous-espace vectoriel de E stable par f et contenant x (cf. Lemme 1.1) est appelé le sous-espace cyclique de f associé à x. Il sera noté $E_{f,x}$.*

Proposition 1.3 – *Soit $x \in E$. Le sous-espace cyclique de f associé à x est*

$$\mathrm{Vect}\{f^i(x),\, i \in \mathbb{N}\}.$$

Démonstration. Posons $V = \mathrm{Vect}\{f^i(x),\, i \in \mathbb{N}\}$. On doit montrer que V est un sous-espace vectoriel de E contenant x, stable par f et inclus dans tout sous-espace vectoriel de E contenant x et stable par f.

Par définition, V est un sous-espace vectoriel de E contenant x. En outre, une récurrence facile assure que V est stable par f.

D'autre part, si W est un sous-espace vectoriel de E contenant x et stable par f, une récurrence facile assure que W contient $f^i(x)$, pour tout $i \in \mathbb{N}$. Ainsi, W contient V.

En conclusion, $V = E_{f,x}$. ■

On est maintenant en position d'introduire la notion, très utile pour la suite, de polynôme minimal *local* d'un endomorphisme.

Remarque 1.4 – Soit $x \in E$.
1. Par définition, le sous-espace vectoriel $E_{f,x}$ est stable par f et on peut donc considérer l'endomorphisme $f_{|E_{f,x}}$ induit par f sur ce sous-espace. D'après la Remarque 2.1 du Chapitre 1, le morphisme d'évaluation en $f_{|E_{f,x}}$ s'exprime alors :

$$\begin{array}{rcccl} \mathrm{ev}_{f_{|E_{f,x}}} & : & \Bbbk[X] & \longrightarrow & \mathrm{End}_{\Bbbk}(E_{f,x}) \\ & & P & \mapsto & P(f)_{|E_{f,x}} \end{array} ;$$

c'est un morphisme d'algèbres.
2. On dispose aussi d'un morphisme d'espaces vectoriels sur $\Bbbk$:

$$\begin{array}{rcccccc} \mathrm{ev}_{f,x} & : & \Bbbk[X] & \xrightarrow{\mathrm{ev}_f} & \mathrm{End}_{\Bbbk}(E) & \longrightarrow & E \\ & & P & \mapsto & P(f) & \mapsto & (P(f))(x) \end{array} .$$

En effet, ev_f est un morphisme d'algèbres, et donc en particulier d'espaces vectoriels. Et, d'autre part, l'application $\mathrm{End}_{\Bbbk}(E) \longrightarrow E$, $g \mapsto g(x)$ est un morphisme d'espaces vectoriels, comme on le vérifie immédiatement.
3. Il n'est pas difficile de monter que

$$\ker\left(\mathrm{ev}_{f_{|E_{f,x}}}\right) = \{P \in \Bbbk[X],\ (P(f))(x) = 0\} = \ker(\mathrm{ev}_{f,x}) \qquad \text{et} \qquad \mathrm{Im}(\mathrm{ev}_{f,x}) = E_{f,x}.$$

(Pour l'identité $\mathrm{Im}(\mathrm{ev}_{f,x}) = E_{f,x}$, on pourra utiliser la Proposition 1.3). Les détails sont laissés en exercice.

Remarque 1.5 –
1. Il est clair que, si E est de dimension finie, alors $\ker\left(\mathrm{ev}_{f_{|E_{f,x}}}\right)$ est un idéal non nul. (Il suffit de raisonner comme pour l'application ev_f en remarquant que $\mathrm{End}_{\Bbbk}(E_{f,x})$ est de dimension finie.) En particulier, si E est de dimension finie, il existe un unique polynôme unitaire $\mu_{f,x}$ dans $\Bbbk[X]$ tel que l'on ait :

$$\ker\left(\mathrm{ev}_{f_{|E_{f,x}}}\right) = \langle \mu_{f,x} \rangle.$$

2. On a que $x = 0$ si et seulement si $\ker\left(\mathrm{ev}_{f_{|E_{f,x}}}\right) = \Bbbk[X]$, c'est-à-dire si et seulement si $\mu_{f,x} = 1$.

Définition 1.6 – *On suppose que E est de dimension finie. L'unique générateur unitaire de l'idéal $\ker\left(\mathrm{ev}_{f_{|E_{f,x}}}\right)$ (cf. Remarque 1.5) est appelé le polynôme minimal local en x de l'endomorphisme f ; il est noté $\mu_{f,x}$.*

Remarque 1.7 – On suppose E de dimension finie. D'après le second point de la Remarque 1.5, $E_{f,x} = (0)$ si et seulement si $x = 0$. Cette même remarque assure que si $x = 0$, alors $\mu_{f,x} = 1$. Si, au contraire, $x \neq 0$, alors $\mu_{f,x}$ n'est autre (par définition) que le polynôme minimale de l'endomorphisme $f_{|E_{f,x}}$ induit sur $E_{f,x}$ par f et il est donc de degré au moins égal à 1.

Remarque 1.8 – On suppose que E est de dimension finie. Pour tout $x \in E$,

$$\mu_{f,x} | \mu_f.$$

Proposition 1.9 – *On suppose que E est de dimension finie. Soient $x \in E$, $\mu_{f,x}$ le polynôme minimal local de f en x et $d = \deg(\mu_{f,x})$. Alors, si x est non nul, la famille $\{f^i(x),\ i \in \mathbb{N},\ 0 \leq i \leq d-1\}$ est une base de $E_{f,x}$.*

Démonstration. Les détails sont laissés en exercice. ∎

Lemme 1.10 – *On suppose que E est de dimension finie. Soit $P \in \Bbbk[X]$ un polynôme irréductible et $k \in \mathbb{N}^*$. Si $x \in \ker((P^k)(f)) \setminus \ker((P^{k-1})(f))$, alors le polynôme minimal local de f en x est P^k.*

Démonstration. On observe pour commencer que, par hypothèse, $x \neq 0$. On a donc $\deg(\mu_{f,x}) \geq 1$ (cf. Remarque 1.7). Par définition du polynôme minimal local en x, $\mu_{f,x} | P^k$. Mais alors, comme P est irréductible, il existe un entier j, $1 \leq j \leq k$ tel que $\mu_{f,x} = P^j$. On a donc $(P^j(f))(x) = (\mu_{f,x}(f))(x) = 0$. Par hypothèse sur x, cela impose que $j = k$. ∎

Proposition 1.11 – *On suppose que E est de dimension finie. Il existe $x \in E$ tel que $\mu_f = \mu_{f,x}$.*

Démonstration. On note μ_f le polynôme minimal de f et on écrit

$$\mu_f = \prod_{1 \leq k \leq N} P_k^{\alpha_k}$$

la décomposition de μ_f en produit de puissances d'irréductibles, où $N \in \mathbb{N}^*$, les $P_1, \ldots, P_N$ sont des polynômes irréductibles deux à deux distincts et $\alpha_1, \ldots, \alpha_N$ des entiers naturels non nuls. D'après le Corollaire 3.3 du Chapitre 1, on a

$$E = \bigoplus_{1 \leq k \leq N} \ker(P_k^{\alpha_k}(f)).$$

D'après le Lemme 3.8 du Chapitre 1, pour tout $1 \leq k \leq N$, on peut considérer $x_k \in \ker(P_k^{\alpha_k}(f)) \setminus \ker(P_k^{\alpha_k - 1}(f))$. On pose

$$x = \sum_{1 \leq k \leq N} x_k.$$

Chacun des sous-espaces $\ker(P_k^{\alpha_k}(f))$, $1 \leq k \leq N$, est stable par f et donc par $\mu_{f,x}(f)$. De l'égalité

$$0 = \mu_{f,x}(f)(x) = \sum_{1 \leq k \leq N} \mu_{f,x}(f)(x_k)$$

on tire donc que, pour $1 \leq k \leq N$,

$$\mu_{f,x}(f)(x_k) = 0.$$

Mais, d'après le Lemme 1.10, le polynôme minimal local de f en x_k est $P_k^{\alpha_k}$. Il découle donc de ce qui précède que, pour $1 \leq k \leq N$:

$$P_k^{\alpha_k} | \mu_{f,x}.$$

Comme les P_k, $1 \leq k \leq N$, sont deux à deux premiers entre eux, on déduit de ce qui précède que

$$\mu_f | \mu_{f,x}.$$

Ceci termine la démonstration, compte tenu de la Remarque 1.8. ■

Définition 1.12 – *On dit que l'endomorphisme f est cyclique s'il existe $x \in E$ tel que $E = E_{f,x}$.*

Définition 1.13 – *Soient $\ell \in \mathbb{N}^*$ et $P = \sum_{0 \leq i \leq \ell-1} c_i X^i + X^\ell$ un polynôme unitaire de $\Bbbk[X]$ de degré ℓ. On appelle matrice compagnon de P la matrice*

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -c_{\ell-1} \end{pmatrix}$$

de $M_\ell(\Bbbk)$.

Remarque 1.14 – On suppose que E est de dimension finie et on note n cette dimension.
1. Supposons que f est cyclique. Par définition, il existe $x \in E$ tel que $E = E_{f,x}$ et on a $x \neq 0$ puisque $E \neq (0)$. D'après la Proposition 1.9, le polynôme minimal local de f en x est de degré n et $\mathcal{B} = \{x, f(x), \ldots, f^{n-1}(x)\}$ est une base de E. Soient alors $a_0, \ldots, a_{n-1} \in \Bbbk$ tels que

$$\mu_{f,x} = X^n - \sum_{0 \leq i \leq n-1} a_i X^i.$$

De l'identité $\mu_{f,x}(f)(x) = 0$, on tire que la matrice de f dans la base $\mathcal{B}$ est

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix}. \tag{2.1}$$

En outre, pour tout $i \in \mathbb{N}$, on a

$$\left(\mu_{f,x}(f)\right)\left(f^i(x)\right) = \left(\mu_{f,x}(f) \circ f^i\right)(x) = \left(f^i \circ \mu_{f,x}(f)\right)(x) = \left(f^i(\mu_{f,x}(f)(x)\right) = f^i(0) = 0.$$

Ainsi, l'endomorphisme $\mu_{f,x}(f)$ s'annule sur une base de E. Il est donc nul. On en déduit que $\mu_f | \mu_{f,x}$ et donc (cf. Remarque 1.8) que

$$\mu_f = \mu_{f,x}.$$

2. Réciproquement, supposons qu'il existe des éléments $a_0, \dots, a_{n-1} \in \Bbbk$ et une base $\mathcal{B}$ tels que la matrice de f dans la base $\mathcal{B}$ soit comme en (2.1). Il est facile de voir que, si l'on note x le premier vecteur de $\mathcal{B}$, on a $E = E_{f,x}$. Ainsi, f est cyclique.
3. Ce qui précède montre qu'un endomorphisme est cyclique si et seulement si il existe une base relativement à laquelle sa matrice est du type (2.1).

Proposition 1.15 – *On suppose que E est de dimension finie et on note n cette dimension. Les assertions suivantes sont équivalentes :*
(i) f est cyclique ;
(ii) $\deg(\mu_f) = \dim(E)$.

Démonstration. Si f est cyclique, le premier point de la Remarque 1.14 assure que $n = \deg(\mu_f)$.

Réciproquement, supposons que $n = \deg(\mu_f)$. La Proposition 1.11 assure l'existence de $x \in E$ tel que $\mu_f = \mu_{f,x}$. Pour un tel x, on a donc $n = \deg(\mu_{f,x})$. Mais, $\deg(\mu_{f,x}) = \dim(E_{f,x})$. On a donc $\dim(E_{f,x}) = \dim(E)$ et pas suite que $E = E_{f,x}$. Ainsi, f est cyclique. ∎

2 Polynôme caractéristique et théorème de Cayley-Hamilton.

Dans cette section, on suppose que E est de dimension finie et on note n cette dimension.

L'objet de cette section est d'introduire le polynôme caractéristique d'un endomorphisme et de démontrer que c'est un polynôme annulateur de cet endomorphisme. Pour cela, il va être utile d'introduire des matrices à coefficients dans l'anneau $\Bbbk[X]$. La remarque suivante définit le cadre approprié de la manière la plus directe possible pour notre objectif. On reviendra sur cette construction plus tard, pour y apporter des compléments utiles pour la suite du cours.

Remarque 2.1 – ***Rappels et compléments de structures : matrices à coefficients dans un anneau.*** Dans cette remarque, A désigne un anneau commutatif intègre.
1. On rappelle qu'alors, on peut construire un corps commutatif $\mathbb{K}$, appelé corps des fractions de A, ayant les propriétés suivantes : il existe un morphisme injectif d'anneaux

$$\iota \quad : \quad A \quad \longrightarrow \quad \mathbb{K} \tag{2.2}$$

tel que, pour tout élément x de $\mathbb{K}$, il existe $(a, b) \in A \times (A \setminus \{0\})$ tel que $x = \iota(a)\iota(b)^{-1}$. Comme le morphisme ι est injectif, il permet d'identifier A à un sous-anneau de $\mathbb{K}$.
2. Soient $p, q \in \mathbb{N}^*$. On note $M_{p,q}(A)$ l'ensemble des matrices à p lignes et q colonnes, à coefficients dans A. Puisqu'on identifie A à un sous-anneau de $\mathbb{K}$, $M_{p,q}(A)$ s'identifie à un sous-ensemble de $M_{p,q}(\mathbb{K})$.

Si $p = q$, on pose $M_p(A) = M_{p,p}(A)$; cet ensemble (vu comme sous-ensemble de $M_p(\mathbb{K})$) est alors un sous-anneau de $M_p(\mathbb{K})$ et on dispose d'une application

$$\det \quad : \quad M_p(A) \quad \longrightarrow \quad A$$

par restriction du déterminant pour les matrices à coefficients dans $\mathbb{K}$.
3. Ce qui précède s'applique en particulier au cas où $A = \Bbbk[X]$. Ainsi, si l'on considère une matrice carrée à coefficients dans $\Bbbk[X]$, on peut lui associer son déterminant, qui est lui-même un élément de $\Bbbk[X]$.

On revient maintenant au contexte du cours.

On rappelle que si $\mathcal{B}$ et $\mathcal{C}$ sont deux bases de E et si $\mathrm{Mat}_{\mathcal{B}}(f)$ et $\mathrm{Mat}_{\mathcal{C}}(f)$ sont les matrices représentatives de f relativement à $\mathcal{B}$ et $\mathcal{C}$ respectivement, il existe une matrice inversible $P \in M_n(\Bbbk)$ telle que

$$\mathrm{Mat}_{\mathcal{C}}(f) = P^{-1}\mathrm{Mat}_{\mathcal{B}}(f)P.$$

Il s'ensuit l'identité

$$\mathrm{Mat}_{\mathcal{C}}(f) - XI_n = P^{-1}\left(\mathrm{Mat}_{\mathcal{B}}(f) - XI_n\right)P$$

dans $M_n(\Bbbk[X])$ qui assure que le déterminant des matrices $\mathrm{Mat}_{\mathcal{B}}(f) - XI_n$ et $\mathrm{Mat}_{\mathcal{C}}(f) - XI_n$ (qui est un élément de $\Bbbk[X]$) coïncident. Ceci justifie la définition suivante.

Définition 2.2 – *On appelle polynôme caractéristique de f le polynôme*

$$\chi_f = (-1)^n \det\left(\mathrm{Mat}_{\mathcal{B}}(f) - XI_n\right),$$

où $\mathcal{B}$ est une base arbitraire de E.

Remarque 2.3 – On suppose que f est cyclique. D'après la Remarque 1.14, il existe une base $\mathcal{B}$ de E relativement à laquelle la matrice de f est

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix}. \tag{2.3}$$

Le polynôme caractéristique de f est donc

$$\chi_f = X^n - \sum_{0 \le i \le n-1} a_i X^i,$$

(cf. Exercice 5.2).

Lemme 2.4 –
1. Si F est un sous-espace vectoriel de E stable par f, alors $\chi_{f_{|F}} | \chi_f$.
2. Si F et G sont des sous-espace vectoriel de E stables par f et supplémentaires, alors $\chi_f = \chi_{f_{|F}}\chi_{f_{|G}}$.

Démonstration. On laisse les détails en exercices. Pour le premier point, on peut considérer une base de F et la compléter en une base de E. La polynôme caractéristique de f est alors le déterminant d'une matrice triangulaire par blocs, ce dont le résultat se déduit. Le second point se traite de manière semblable en considérant une base adaptée à la décomposition $E = F \oplus G$. ∎

Proposition 2.5 – *Les assertions suivantes sont équivalentes :*
(i) f est cyclique ;
(ii) $\chi_f = \mu_f$.
En particulier, si f est cyclique, $\chi_f(f) = 0$.

Démonstration. On suppose que f est cyclique et on reprend les notations de la Remarque 1.14. Cette Remarque montre que

$$\mu_f = X^n - \sum_{0\leq i\leq n-1} a_i X^i.$$

Par ailleurs, la Remarque 2.3 assure que

$$\chi_f = X^n - \sum_{0\leq i\leq n-1} a_i X^i.$$

Donc

$$\chi_f = \mu_f.$$

Réciproquement, si $\chi_f = \mu_f$, la Proposition 1.15 assure que f est cyclique. ■

Théorème 2.6 ***(Théorème de Cayley-Hamilton)*** *On a* $\chi_f(f) = 0$.

Démonstration. Soit $x \in E$. On considère le sous-espace cyclique $E_{f,x}$ de f associé à x et l'endomorphisme g induit par f sur $E_{f,x}$. Bien sûr, g est cyclique. La Proposition 2.5 assure donc que $\chi_g(g) = 0$. En particulier, $0 = \chi_g(g)(x) = \chi_g(f)(x)$. Mais, d'après le Lemme 2.4, $\chi_g|\chi_f$. Donc $\chi_f(f)(x)$.

Ainsi, pour tout x dans E, $\chi_f(f)(x) = 0$. Autrement dit, $\chi_f(f) = 0$. ■

Remarque 2.7 – Il découle du Théorème de Cayley-Hamilton que le degré du polynôme minimal de f est majoré par la dimension de E.

Remarque 2.8 – On note χ_f le polynôme caractéristique de f et on écrit

$$\chi_f = \prod_{1\leq k\leq N} P_k^{\beta_k}$$

la décomposition de χ_f en produit de puissances d'irréductible, où $N \in \mathbb{N}^*$, les $P_1, \ldots, P_N$ sont des polynômes irréductibles deux à deux distincts et $\beta_1, \ldots, \beta_N$ des entiers naturels non nuls. D'après le Théorème de Cayley-Hamilton, il existe des entiers α_k, $1 \leq k \leq N$, vérifiant $0 \leq \alpha_k \leq \beta_k$ et tels que

$$\mu_f = \prod_{1\leq k\leq N} P_k^{\alpha_k}.$$

Bien sûr, pour $1 \leq k \leq N$, $(0) \subseteq \ker(P_k^{\alpha_k}(f)) \subseteq \ker(P_k^{\beta_k}(f))$. En fait, le second point du Lemme 3.8 du Chapitre 1 assure que

$$\ker(P_k^{\alpha_k}(f)) = \ker(P_k^{\beta_k}(f)).$$

3 Réduction de Frobenius.

Dans cette section, on suppose que E est de dimension finie.

La réduction de Frobenius de l'endomorphisme f est le contenu du Théorème 3.5. C'est l'objectif majeur de cette section.

Pour l'atteindre, on passe par la Proposition 3.3. On rappelle que, conformément à la Proposition 1.11, il existe un élément x de E tel que $\mu_f = \mu_{f,x}$. La Proposition 3.3 démontre que si x est un tel élément, alors le sous-espace $E_{f,x}$ (qui est stable par f) admet un supplémentaire qui est aussi stable par f. La démonstration de cette proposition est difficile et on passe par un lemme préparatoire dans lequel on établit un lien entre $E_{f,x}$ et un certain sous-espace cyclique de E^* associé a la transposée de f. C'est ce lemme qui contient la difficulté technique.

On commence par un rappel sur les notions de dualité qui nous seront utiles.

Remarque 3.1 – On note E^* l'espace dual de E. Ainsi, E^* est l'espace vectoriel des formes linéaires sur E : $E^* = \mathrm{Hom}_{\Bbbk}(E, \Bbbk)$.
1. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Soit $1 \leq i \leq n$, on note e_i^* la forme linéaire sur E définie par

$$e_i^*(e_j) = \delta_{ij}.$$

(Ci-dessus, δ_{ij} est le symbole de Kronecker : il vaut 1 lorsque $i = j$ et 0 lorsque $i \neq j$.) La forme linéaire e_i^* est appelée i-ème *forme coordonnée* puisque, si x est un vecteur de E, $e_i^*(x)$ est la coordonnée de e_i dans la décomposition de x relative à la base $\mathcal{B}$. Il n'est pas difficile, alors, de vérifier que la famille $(e_1^*, \ldots, e_n^*)$ est une base de E^*, appelée *base duale* de la base $\mathcal{B}$ et notée $\mathcal{B}^*$.

Réciproquement, si $\mathcal{C}$ est une base de E^*, il existe une unique base de E dont $\mathcal{C}$ est la duale. L'unique base de E dont $\mathcal{C}$ est la duale est parfois appelée *base ante-duale* de $\mathcal{C}$.
2. Si F est un sous-espace de E^*, on note $F^\perp$ l'orthogonal de F (au sens de la dualité). Par définition, $F^\perp$ est l'ensemble des éléments de E qui sont dans le noyau de toutes les formes linéaires appartenant à F :

$$F^\perp = \{x \in E \,|\, \varphi(x) = 0, \forall\, \varphi \in F\}.$$

Soit alors $p = \dim_{\Bbbk}(F)$, $0 \leq p \leq n$. Si $(\phi_1, \ldots, \phi_p)$ est une base de F et si l'on complète cette base en une base $(\phi_1, \ldots, \phi_n)$ de E^*, on peut considérer la base ante-duale de $(\phi_1, \ldots, \phi_n)$: $\mathcal{B} = \{f_1, \ldots, f_n\}$. Une vérification facile montre que les vecteurs $f_{p+1}, \ldots, f_n$ forment une base de $F^\perp$. En particulier, on a

$$\dim_{\Bbbk}\left(F^\perp\right) = \dim_{\Bbbk}(E) - \dim_{\Bbbk}(F).$$

3. A tout endomorphisme g de E, on peut associer l'application, dite *transposée* de g :

$$\begin{array}{cccc} {}^t g & : & E^* & \longrightarrow & E^* \\ & & \varphi & \mapsto & \varphi \circ g \end{array}.$$

Il est facile de vérifier que ${}^t g$ est une application linéaire de E^* : ${}^t g \in \mathrm{End}_{\Bbbk}(E^*)$. On a donc une application

$$\begin{array}{ccccc} {}^t(-) & : & \mathrm{End}_{\Bbbk}(E) & \longrightarrow & \mathrm{End}_{\Bbbk}(E^*) \\ & & g & \mapsto & {}^t g \end{array}.$$

Il est facile de vérifier que cette application est linéaire. De plus, si $g, h \in \mathrm{End}_{\Bbbk}(E)$, alors ${}^t(g \circ h) = {}^t h \circ {}^t g$.

Lemme 3.2 – *On suppose que E est de dimension finie égale à $n \in \mathbb{N}^*$. Soit x est un élément de E tel que $\mu_f = \mu_{f,x}$, et p le degré de μ_f. Pour $0 \leq i \leq p-1$, on pose $e_i = f^i(x)$, on complète la famille libre (cf. Proposition 1.9) $(e_0, \ldots, e_{p-1})$ en une base $\mathcal{B} = (e_0, \ldots, e_{n-1})$ de E et on note $\mathcal{B}^* = (e_0^*, \ldots, e_{n-1}^*)$ sa base duale. Alors, la famille $(({}^t f)^j(e_{p-1}^*),\, 0 \leq j \leq p-1)$ est une base de l'espace cyclique $E^*_{{}^t f, e_{p-1}^*}$ associé à ${}^t f$ et e_{p-1}^*.*

Démonstration. Observons que l'hypothèse $\mu_f = \mu_{f,x}$ assure que x est non nul.

D'après le Lemme 1.9, la famille $(e_0, \ldots, e_{p-1})$ est une base de $E_{f,x}$ (en particulier, elle est libre). On considère alors l'endomorphisme transposé de f :

$$\begin{array}{ccccc} {}^t f & : & E^* & \longrightarrow & E^* \\ & & \varphi & \mapsto & \varphi \circ f \end{array}$$

et le sous-espace cyclique de ${}^t f$ associé à e_{p-1}^* :

$$E^*_{{}^t f, e_{p-1}^*} = \mathrm{Vect}\{({}^t f)^j(e_{p-1}^*),\, j \in \mathbb{N}\}.$$

Comme μ_f est de degré p, d'après la Proposition 2.7 du Chapitre 1, on a $\Bbbk[f] = \mathrm{Vect}\{f^j,\, 0 \leq j \leq p-1\}$. En d'autres termes : pour tout $i \in \mathbb{N}$, f^i est combinaison linéaire de $\mathrm{id}_E, f, \ldots, f^{p-1}$. Il s'ensuit, d'après le point 3 de la Remarque 3.1, que, pour tout $i \in \mathbb{N}$, $({}^t f)^i$ est combinaison linéaire de $\mathrm{id}_{E^*}, {}^t f, \ldots, {}^t(f^{p-1})$. On a donc

$$E^*_{{}^t f, e_{p-1}^*} = \mathrm{Vect}\{({}^t f)^j(e_{p-1}^*),\, 0 \leq j \leq p-1\}. \tag{2.4}$$

Considérons à présent la famille

$$\left((e_{p-1}^*, {}^tf(e_{p-1}^*), \ldots, ({}^tf)^{p-1}(e_{p-1}^*)\right)$$

d'éléments de $E^*_{{}^tf,e^*_{p-1}}$. Soient $\lambda_0, \ldots, \lambda_{p-1}$ des éléments de $\Bbbk$ tels que

$$\lambda_0 e_{p-1}^* + \lambda_1 {}^tf(e_{p-1}^*) + \ldots + \lambda_{p-1}({}^tf)^{p-1}(e_{p-1}^*) = 0.$$

L'identité ci-dessus appliquée à e_0 donne $\lambda_{p-1} = 0$. Puis, la même identité appliquée à e_1 donne $\lambda_{p-2} = 0$. En continuant ainsi jusqu'à e_{p-1}, on trouve que les λ_i, $0 \leq i \leq p-1$, sont nuls. Ainsi, la famille ci-dessus est libre. Mais, l'égalité (2.4) montre qu'elle est génératrice de $E^*_{{}^tf,e^*_{p-1}}$. Ceci termine la démonstration. ∎

Proposition 3.3 – *On suppose que E est de dimension finie. Si x est un élément de E tel que $\mu_f = \mu_{f,x}$, alors $E_{f,x}$ admet un supplémentaire stable par f.*

Démonstration. On reprend les notations du Lemme 3.2 et de sa démonstration. Nous allons montrer que l'orthogonal de $E^*_{{}^tf,e^*_{p-1}}$ (au sens de la dualité) est un supplémentaire de $E_{f,x}$, stable par f. Par définition, cet orthogonal est

$$\left(E^*_{{}^tf,e^*_{p-1}}\right)^{\perp} = \left\{y \in E \mid \forall j \in \mathbb{N},\, ({}^tf)^j(e_{p-1}^*)(y) = 0\right\} = \left\{y \in E \mid \forall j \in \mathbb{N},\, e_{p-1}^* \circ f^j(y) = 0\right\}.$$

1. La stabilité de ce sous-espace par f est immédiate.
2. Soit ensuite $y \in \left(E^*_{{}^tf,e^*_{p-1}}\right)^{\perp} \cap E_{f,x}$. Comme $y \in E_{f,x}$, il existe $\lambda_i \in \Bbbk$, $0 \leq i \leq p-1$, tel que

$$y = \sum_{0 \leq i \leq p-1} \lambda_i e_i = \sum_{0 \leq i \leq p-1} \lambda_i f^i(x).$$

Et, pour $j \in \mathbb{N}$, on a

$$0 = e_{p-1}^* \circ f^j(y)$$

puisque $y \in \left(E^*_{{}^tf,e^*_{p-1}}\right)^{\perp}$. En appliquant cette observation avec $j = 0$, on obtient que $\lambda_{p-1} = 0$. Puis, en appliquant cette observation avec $j = 1$, on obtient que $\lambda_{p-2} = 0$. En procédent ainsi jusqu'à $j = p-1$, on conclut que $y = 0$.
3. Ce qui précède montre que l'on a une somme directe de sous-espaces stables par f comme suit :

$$E_{f,x} \bigoplus \left(E^*_{{}^tf,e^*_{p-1}}\right)^{\perp} \subseteq E. \tag{2.5}$$

Mais, d'après le Lemme 3.2, $\dim\left(E^*_{{}^tf,e^*_{p-1}}\right) = p$ et donc, d'après le deuxime point de la Remarque 3.1, $\dim\left((E^*_{{}^tf,e^*_{p-1}})^{\perp}\right) = n - p$. En comparant les dimensions dans l'inclusion (2.5), on obtient que cette inclusion est une égalité. Ceci termine la démonstration. ∎

On est maintenant en position de démontrer l'existence de la décomposition de Frobenius (Théorème 3.5). La partie *existence* de cette démonstration est simple. La partie *unicité* est plus délicate. Pour préparer cette dernière, on énonce sous forme d'exercice un résultat élémentaire qui y sera utile.

Exercice 3.4 – Soient F et G deux espaces vectoriels sur $\Bbbk$, de dimension finie, u un endomorphisme de F et v un endomorphisme de G. S'il existe une base $\mathcal{B}$ de F et une base $\mathcal{C}$ de G telles que $\mathrm{Mat}_{\mathcal{B}}(u) = \mathrm{Mat}_{\mathcal{C}}(g)$, alors il existe un isomorphisme $\varphi : F \longrightarrow G$ d'espaces vectoriels tel que $v = \varphi \circ u \circ \varphi^{-1}$.

Théorème 3.5 – ***Réduction de Frobenius.*** *Il existe $r \in \mathbb{N}^*$, une suite $P_1, \ldots, P_r$ de polynômes unitaires de $\Bbbk[X]$ et des sous-espaces $E_1, \ldots, E_r$ de E, stables par f et non nuls tels que :*
1. $P_r | \ldots | P_2 | P_1$;
2. $E = E_1 \oplus \ldots \oplus E_r$;
3. pour tout $i \in \{1, \ldots, r\}$, la restriction de f à E_i est cyclique de polynôme minimal P_i.
De plus, l'entier r et la suite $P_1, \ldots, P_r$ sont uniques.
Enfin, $\mu_f = P_1$ et, pour $1 \leq i \leq r$, $\deg(P_i) = \dim(E_i)$.

Démonstration. On commence par démontrer l'existence.

On procède par récurrence sur la dimension de l'espace vectoriel E. Si E est de dimension 1, le résultat est évident (avec $r = 1$, $P_1 = \mu_f$ et $E_1 = E$). On le suppose vrai pour tout espace vectoriel de dimension n et on considère un espace de dimension $n+1$. D'après la Proposition 1.11 du Chapitre 1 et la Proposition 3.3, il existe un élément $x \in E$, $x \neq 0$, et un sous-espace F de E stable par E tels que $\mu_f = \mu_{f,x}$ et

$$E = E_{f,x} \bigoplus F.$$

Bien sûr, la restriction de f à $E_{f,x}$ est un endomorphisme cyclique de $E_{f,x}$. Si $F = 0$, le résultat est clair (avec $r = 1$, $E = E_1$ et $\mu_f = P_1$). Sinon, l'hypothèse de récurrence appliquée à $f_{|F}$ assure l'existence de $r \in \mathbb{N}$, $r \geq 2$, de polynômes unitaires $P_2, \ldots, P_r$ et de sous-espaces vectoriels $E_2, \ldots, E_r$ de F, stables par f, tels que $P_r|\ldots|P_2$, $F = E_2 \oplus \ldots \oplus E_r$ et, pour tout $i \in \{2, \ldots, r\}$, la restriction de f à E_i est cyclique de polynôme minimal P_i. Posons alors $E_1 = E_{f,x}$ et $P_1 = \mu_{f_{|E_{f,x}}}$. On a bien sûr que

$$E = E_1 \oplus \ldots \oplus E_r.$$

Notons f_i la restriction de f à E_i, $1 \leq i \leq r$. Il est clair aussi que les f_i, $1 \leq i \leq r$, sont cycliques et de polynôme minimal P_i. On a

$$P_1 = \mu_{f_{|E_{f,x}}} = \mu_{f,x} = \mu_f.$$

(La première égalité est la définition de P_1, la deuxième est la d'efinition du polynôme minimal local et la troisième est vrair par définition de x.) Comme P_1 est annulateur de f, il est annulateur de f_2 et donc $P_2|P_1$. Ceci démontre la partie *existence* de l'énoncé.

Pour établir l'unicité, on commence par une observation. Supposons donnés r, une suite $P_1, \ldots, P_r$ et une suite $E_1, \ldots, E_r$ comme dans l'énoncé et, pour $1 \leq i \leq r$, notons f_i l'endomorphisme de E_i induit par f. Comme P_1 est multiple de tous les P_i, $1 \leq i \leq r$, P_1 est annulateur de f_i pour $1 \leq i \leq r$. Donc P_1 est annulateur de f, c'est à dire que $\mu_f|P_1$. Mais, μ_f est annulateur de f_1, donc $P_1|\mu_f$. On a donc $\mu_f = P_1$.

D'autre part, pour $1 \leq i \leq r$, f_i est un endomorphisme cyclique de E_i de polynôme minimal P_i et donc $\deg(P_i) = \dim_{\Bbbk}(E_i)$ (cf. Proposition 1.15).

On démontre à présent l'unicité. Supposons donnés des entiers strictement positifs r, s, des suites $P_1, \ldots, P_r$ et $Q_1, \ldots, Q_s$ de polynômes unitaires et des suites $F_1, \ldots, F_r$ et $G_1, \ldots, G_s$ de sous-espaces vectoriels de E stables par f et non nuls tels que $P_r|\ldots|P_2|P_1$, $Q_s|\ldots|Q_2|Q_1$,

$$E = \bigoplus_{1 \leq i \leq r} F_i, \quad E = \bigoplus_{1 \leq i \leq s} G_i$$

et tels qu'enfin, pour $1 \leq i \leq r$, l'endomorphisme f_i induit par f sur F_i soit cyclique de polynôme minimal P_i et, pour $1 \leq j \leq s$, l'endomorphisme g_j induit par f sur G_j soit cyclique de polynôme minimal Q_j. On peut supposer, sans perte de généralité, que $r \leq s$.

L'observation qui précède montre que

$$P_1 = \mu_f = Q_1$$

et que

$$\sum_{1 \leq i \leq r} \deg(P_i) = \dim_{\Bbbk}(E) = \sum_{1 \leq j \leq s} \deg(Q_j). \tag{2.6}$$

Supposons que l'ensemble $\{i \in \mathbb{N},\ 2 \leq i \leq r \,|\, P_i \neq Q_i\}$ soit non vide et soit k son plus petit élément. On pose

$$\pi = P_k(f).$$

Comme f stabilise les sous-espaces F_i, $1 \leq i \leq r$, et G_j, $1 \leq j \leq s$, π les stabilise aussi et on a :

$$\bigoplus_{1 \leq i \leq r} \pi(F_i) = \pi(E) = \bigoplus_{1 \leq j \leq s} \pi(G_j).$$

Mais, $\pi = P_k(f)$ s'annule sur tout F_i, $i \geq k$, car pour un tel i, P_k est un multiple du polynôme minimal P_i de f_i. Donc

$$\bigoplus_{1\leq i\leq k-1} \pi(F_i) = \pi(E) = \bigoplus_{1\leq j\leq s} \pi(G_j). \tag{2.7}$$

Soit à présent $1 \leq i \leq k-1$. Par définition de k, $P_i = Q_i$. Il s'ensuit que $\dim_{\Bbbk}(F_i) = \dim_{\Bbbk}(G_i)$ et qu'il existe une base $\mathcal{B}_i$ de F_i et une base $\mathcal{C}_i$ de G_i telles que $\mathrm{Mat}_{\mathcal{B}_i}(f_i) = \mathrm{Mat}_{\mathcal{C}_i}(g_i)$ (cf. Remarque 1.14). Il existe donc (cf. Exercice 3.4) un isomorphisme $\varphi_i : F_i \longrightarrow G_i$ tel que $g_i = \varphi_i \circ f_i \circ \varphi_i^{-1}$ et donc $P_k(g_i) = \varphi_i \circ P_k(f_i) \circ \varphi_i^{-1}$. On a donc :

$$\pi(G_i) = P_k(f)(G_i) = P_k(g_i)(G_i) = \varphi_i \circ P_k(f_i) \circ \varphi_i^{-1}(G_i) = \varphi_i \circ P_k(f_i)(F_i) = \varphi_i \circ P_k(f)(F_i) = \varphi_i \circ \pi(F_i).$$

En particulier, pour $1 \leq i \leq k-1$,

$$\dim(\pi(F_i)) = \dim(\pi(G_i)).$$

On déduit de cela et de l'identité (2.7) que :

$$\text{pour} \quad j \geq k, \qquad \pi(G_j) = 0.$$

En particulier, $P_k(f)$ annule G_k et donc $Q_k|P_k$. Mais, en considérant $\rho = Q_k(f)$ au lieu de π, un argument semblable montre que $P_k|Q_k$. On aboutit donc à $P_k = Q_k$, ce qui est absurde.

Ce qui précède montre que, pour $1 \leq i \leq r$, $P_i = Q_i$. La relation (2.6) montre alors que, si $r \leq j < s$, $\deg(Q_j) = 0$. Or, Q_j ne peut être constant puisque c'est le polynôme minimal d'un endomorphisme d'un espace non nul. C'est donc qu'un tel j n'existe pas, autrement dit que $r = s$. Comme avec ce qui précède on a $P_i = Q_i$ pour $1 \leq i \leq r$, on a prouvé l'unicité. ■

Définition 3.6 – *On reprend les notations du Théorème 3.5. Les polynômes $P_1, \ldots, P_r$ sont appelés les invariants de similitude de l'endomorphisme f.*

Remarque 3.7 – On reprend les notations du Théorème 3.5. Ainsi, on dispose de $r \in \mathbb{N}^*$, une suite $P_1, \ldots, P_r$ de polynômes unitaires de $\Bbbk[X]$ et des sous-espaces stables $E_1, \ldots, E_r$ non nuls de E tels que $P_r|\ldots|P_2|P_1$, $E = E_1 \oplus \ldots \oplus E_r$ et, pour tout $i \in \{1, \ldots, r\}$, la restriction de f à E_i est cyclique de polynôme minimal P_i.

1. Pour $1 \leq i \leq r$, E_i est non nul. Il s'ensuit que P_i ne peut être constant : il est le polynôme minimal d'un endomorphisme d'un espace non nul.
2. Pour $1 \leq i \leq r$, l'endomorphisme induit par f sur E_i est cyclique de polynôme minimal P_i. Les résultats de la Section 1 assurent donc qu'il existe une base de E_i relativement à laquelle la matrice de cet endomorphisme est la matrice compagnon de P_i : C_{P_i}.
3. Il découle de ce qui précède qu'il existe une base de E relativement à laquelle la matrice de l'endomorphisme est la matrice diagonale par bloc dont les blocs successifs sont les matrices compagnon $C_{P_1}, \ldots, C_{P_r}$.
4. Le Théorème 3.5 assure que $\mu_f = P_1$. En outre, le point 3 ci-dessus assure que

$$\chi_f = P_1 \ldots P_r$$

(cf. Remarque 2.3 et Lemme 2.4).

Remarque 3.8 – **Facteurs irréductibles des polynômes minimaux et caractéristiques.** Le but de la présente remarque est de comparer les facteur irréductibles de μ_f et de χ_f.

1. Comme $\mu_f|\chi_f$, par le Théorème de Cayley-Hamilton, il est clair que tout facteur irréductible de μ_f est aussi un facteur irréductible de χ_f.
2. Utilisons maintenant la Remarque 3.7 en reprenant ses notations. En particulier, le polynômes $P_1, \ldots, P_r$ sont les invariants de similitude de f, et on a :

$$P_r|\ldots|P_2|P_1\,, \qquad \mu_f = P_1 \quad \text{et} \quad \chi_f = P_1 \ldots P_r.$$

Si Q est un facteur irréductible de χ_f, l'identité $\chi_f = P_1 \ldots P_r$ assure qu'il existe $1 \leq i \leq r$ tel que $Q|P_i$. Mais en outre, $P_i|P_1 = \mu_f$. On en déduit que Q divise μ_f et donc que c'est un facteur irréductible de μ_f.

3. On a montré que les facteur irréductibles de μ_f et χ_f sont les mêmes.

La terminologie de la Définition 3.6 est justifiée par la proposition suivante. On rappelle que, si F est un espace vectoriel sur $\Bbbk$, deux endomorphismes u et v de F sont dits *semblables* s'il existe $\sigma \in \mathrm{Aut}_{\Bbbk}(F)$ tel que $v = \sigma \circ u \circ \sigma^{-1}$.

Proposition 3.9 – *Deux endomorphismes de E sont semblables si et seulement si ils ont les mêmes invariants de similitude.*

Démonstration. On laisse la démonstration en exercice. On pourra utiliser la Remarque 3.7 et l'Exercice 3.4. ∎

4 Calcul effectif des invariants de similitude.

Dans cette section, on met en évidence un moyen effectif de calcul des invariants de similitude. Pour cela, on commence par l'étude des matrices à coefficients dans un anneau euclidien.

4.1 Matrices à coefficients dans un anneau euclidien.

Dans cette section, A désigne un anneau commutatif intègre, A^* le groupe de ses éléments inversibles et $\mathbb{K}$ son corps des fractions. On identifie A à un sous-anneau de $\mathbb{K}$. (Voir le premier point de la Remarque 2.1.) Soient $p, q \in \mathbb{N}^*$. On note $M_{p,q}(A)$ l'ensemble des matrices à p lignes et q colonnes, à coefficients dans A. On l'identifie à un sous-ensemble de $M_{p,q}(\mathbb{K})$. (Voir le deuxième point de la Remarque 2.1.) Pour $1 \leq i \leq p$ et $1 \leq j \leq q$, on note E_{ij} la matrice dont tous les coefficients sont nuls excepté celui situé sur la ligne i et la colonne j qui vaut 1.

Si $p = q$, on pose $M_p(A) = M_{p,p}(A)$; cet ensemble est un sous-anneau de $M_p(\mathbb{K})$ dont le groupe des unités est noté $\mathrm{GL}_p(A)$. On rappelle (cf. Remarque 2.1) qu'on dispose d'une application

$$\det \ : \ M_p(A) \ \longrightarrow \ A$$

par restriction du déterminant pour les matrices à coefficients dans $\mathbb{K}$. Il est clair alors que $\mathrm{GL}_p(A)$ est l'ensemble des matrices de $M_p(A)$ de déterminant inversible dans A :

$$\mathrm{GL}_p(A) = \{X \in M_p(A) \,|\, \det(X) \in A^*\}.$$

On pose en outre

$$\mathrm{SL}_p(A) = \{X \in M_p(A) \,|\, \det(X) = 1\}.$$

Par ailleurs, pour tous $1 \leq i \neq j \leq p$ et pour tout $\lambda \in A$, on pose $B_{ij}(\lambda) = I_p + \lambda E_{ij}$. Il est clair que, pour tous $1 \leq i \neq j \leq p$ et pour tout $\lambda \in A$, $B_{ij}(\lambda) \in \mathrm{SL}_p(A)$. Enfin, pour tout élément $\sigma \in \mathfrak{S}_p$, la matrice de permutation P_σ associée à σ est un élément de $\mathrm{GL}_p(A)$.

On appelle opération élémentaire sur les lignes d'une matrice X de $M_{p,q}(A)$ toute opération qui consiste à permuter deux lignes de X ou à remplacer une ligne de X par la somme de cette ligne et d'un multiple à coefficient dans A d'une autre ligne. On définit de la même façon les opérations élémentaires sur les colonnes d'une matrice. Enfin, on appelle opérations élémentaires sur une matrice X de $M_{p,q}(A)$ toute opération élémentaire sur les lignes ou sur les colonnes de X. Il est facile de voir qu'effectuer une opération élémentaire sur les lignes (resp. les colonnes) d'une matrice $X \in M_{p,q}(A)$ revient à la multiplier à gauche (resp. à droite) par une matrice de permutation ou par une matrice $B_{ij}(\lambda)$.

On rappelle la définition suivante.

Définition 4.1.1 – *L'anneau commutatif intègre A est dit* euclidien *s'il existe une application (appelée stathme euclidien)*

$$\varphi \,:\, A \setminus \{0\} \longrightarrow \mathbb{N}$$

vérifiant la propriété suivante : pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $(q, r) \in A \times A$ tel que $a = bq + r$ et, ou bien $r \neq 0$ et $\varphi(r) < \varphi(b)$, ou bien $r = 0$.

Exemple 4.1.2 – Les exemples suivants sont bien connus.
1. L'anneau $\mathbb{Z}$ muni du stathme $\varphi : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$, $z \mapsto |z|$, est un anneau euclidien.
2. Pour tout corps commutatif $\Bbbk$, l'anneau $\Bbbk[X]$ muni du stathme $\varphi : \Bbbk[X] \setminus \{0\} \longrightarrow \mathbb{N}$, $P \mapsto \deg(P)$, est un anneau euclidien.
3. Tout corps commutatif $\Bbbk$ muni d'une application quelconque $\varphi : \Bbbk \setminus \{0\} \longrightarrow \mathbb{N}$, est un anneau euclidien.

Le résultat suivant est essentiel.

Proposition 4.1.3 – *On suppose A euclidien et on note $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ son stathme. Soient $p, q \in \mathbb{N}^*$ et X une matrice $p \times q$ à coefficients dans A, non nulle et de rang r comme matrice à coefficients dans $\mathbb{K}$. Il existe des matrices $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$ et des éléments $a_1, \ldots, a_r$ non nuls de A vérifiant $a_1 A \supseteq \ldots \supseteq a_r A$ tels que PXQ soit la matrice $(a_{ij})_{1 \leq i \leq p, 1 \leq j \leq q}$, où $a_{ii} = a_i$ pour $1 \leq i \leq r$ et $a_{ij} = 0$ sinon.*

Démonstration. Elle se fait par une fastidieuse récurrence que l'on passe sous silence au profit de la description d'un processus algorithmique effectif de calcul. ∎

Un algorithme de réduction pour les matrices à coefficients dans un anneau euclidien. On suppose A euclidien et on note $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ son stathme.

Pour tout $Y \in M_{p,q}(A) \setminus \{0\}$. On note $\delta(Y)$ la plus petite valeur prise par φ sur les coefficients non nuls de Y. Ceci définit une application

$$\delta : M_{p,q}(A) \setminus \{0\} \longrightarrow \mathbb{N}.$$

Soit $X \in M_{p,q}(A) \setminus \{0\}$. Le processus algorithmique qui suit va consister à effectuer des transformations successives sur les lignes et les colonnes de X, juqu'à obtenir une nouvelle matrice, de la forme prevue par la Proposition 4.1.3. Afin de ne pas alourdir les notations, on notera parfois de la même façon une matrice et celle obtenue en effectuant une opération élémentaire sur celle-ci. On remarque que, si la matrice Y est non nulle, toute opération élémentaire sur Y produit une matrice non nulle.

Étape 1 : Par transformations élémentaires, on construit une nouvelle matrice non nulle $X = (x_{ij}) \in M_{p,q}(A)$ telle que $\delta(X) = \varphi(x_{11})$.

Étape 2 : Si l'un des termes sur la première ligne (resp. la première colonne) de X autre que le terme en position $(1, 1)$ n'est pas divisible par x_{11}, par transformation élémentaire, on peut construire une nouvelle matrice X dans laquelle la colonne (resp. ligne) de ce terme a été modifiée de sorte que le terme en question soit remplacé par son reste (non nul) dans sa division euclidienne par x_{11}.

La nouvelle matrice a une image par δ strictement inférieure à celle de la précédente. On réitère sur cette dernière l'étape 1 puis l'étape 2.

Comme les valeurs possibles pour l'image de δ sont minorées par 0, un tel processus s'arrête nécessairement après un nombre fini d'étapes. Ainsi, au bout d'un nombre fini d'étapes, on obtient une matrice X telle que $\delta(X) = x_{11}$ et telle que x_{11} divise tous les termes qui sont en première ligne ou première colonne.

Par opérations élémentaires à nouveau, on peut la transformer en une matrice X dont le terme en position $(1, 1)$ est non nul et dans laquelle tous les autres termes qui sont en première ligne ou première colonne sont nuls. L'image par δ de cette nouvelle matrice est au plus égal à celle de la précédente.

Étape 3 : La matrice obtenue à l'étape précédente satisfait $x_{1k} = x_{k1} = 0$ pour $k > 1$. S'il existe parmi les termes situés en dehors de sa première ligne et de sa première colonne un terme qui n'est pas divisible par x_{11}, on ajoute à la première ligne de X la ligne où figure ce terme. Il s'agit d'une transformation élémentaire qui laisse stable la valeur de δ. On observe que cela place sur la première ligne un terme qui n'est pas divisible par le terme en position $(1, 1)$. On applique alors à cette matrice les étapes 1 et 2 ci-dessus. L'observation ci-dessus montre que ceci a pour effet de faire strictement chuter la valeur prise par δ. Pour cette raison, en un nombre fini d'étapes, on obtient une matrice telle que $x_{1k} = x_{k1} = 0$ pour $k > 1$ et $x_{11} | x_{i,j}$, pour tous i, j.

A ce stade, une observation est utile. Si $Z \in M_{p,q}(A)$ est une matrice dont tous les coefficients sont divisibles par un élément non nul α de A, toute matrice obtenue à partir de Z par opérations élémentaires a tous ses coefficients divisibles par α.

L'algorithme précédent produit par transformations élémentaires, à partir d'une matrice non nulle X de $M_{p,q}(A)$, une matrice $Y = (y_{ij})$ telle que y_{11} divise tous les coefficients de Y et dont tous les coefficients en première ligne ou première colonne sont nuls sauf y_{11}. On peut alors l'appliquer à nouveau à la sous-matrice de Y obtenue en effaçant la première ligne et la première colonne. Compte tenu de l'observation ci-dessus, on construira ainsi une matrice

$$\begin{pmatrix} y_{11} & 0 & \dots & \dots & 0 \\ 0 & y_{22} & 0 & \dots & 0 \\ 0 & 0 & y_{3,3} & \dots & y_{3,m} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & y_{n,3} & \dots & y_{n,m} \end{pmatrix}$$

dont tous les coefficients sont divisibles par y_{11}. Il est clair alors qu'en continuant de la sorte on aboutit à une matrice du type décrit dans la Proposition 4.1.3.

La proposition suivante étudie l'unicité de la suite finie $a_1, \dots, a_r$ de la Proposition 4.1.3. Il est clair que la longueur de cette suite (c'est à dire l'entier r) est unique puisqu'il est égal au rang de la matrice (vue comme matrice à coefficients dans le corps commutatif $\mathbb{K}$).

Proposition 4.1.4 – *On suppose A euclidien. Soient $p, q \in \mathbb{N}^*$ des entiers et X une matrice $p \times q$ à coefficients dans A, non nulle et de rang r comme matrice à coefficients dans $\mathbb{K}$.*
1. On suppose donnés des matrices $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$ et des éléments $a_1, \dots, a_r$ non nuls de A vérifiant $a_1A \supseteq \dots \supseteq a_rA$ tels que PXQ soit la matrice $(a_{ij})_{1\leq i\leq p, 1\leq j\leq q}$ où, $a_{ii} = a_i$ pour $1 \leq i \leq r$ et $a_{ij} = 0$ sinon. Alors, pour $1 \leq k \leq \min\{p, q\}$, l'idéal de A engendré par les mineurs $k \times k$ de A est $\langle a_1 \dots a_k\rangle$ si $k \leq r$ et est nul si $k > r$.
2. On suppose donnés, d'une part, $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$ et des éléments $a_1, \dots, a_r$ non nuls de A vérifiant $a_1A \supseteq \dots \supseteq a_rA$ tels que PXQ soit la matrice $(a_{ij})_{1\leq i\leq p, 1\leq j\leq q}$ où, $a_{ii} = a_i$ pour $1 \leq i \leq r$ et $a_{ij} = 0$ sinon et, d'autre part, $P' \in \mathrm{GL}_p(A)$, $Q' \in \mathrm{GL}_q(A)$ et des éléments $a'_1, \dots, a'_r$ non nuls de A vérifiant $a'_1A \supseteq \dots \supseteq a'_rA$ tels que $P'XQ'$ soit la matrice $(b_{ij})_{1\leq i\leq p, 1\leq j\leq q}$ où, $b_{ii} = a'_i$ pour $1 \leq i \leq r$ et $b_{ij} = 0$ sinon. Alors, il existe des éléments inversibles $u_1, \dots, u_r$ de A tels que, pour $1 \leq k \leq r$, $a'_i = u_ia_i$.

Démonstration. On donne une idée de la démonstration, les détails sont laissés en exercice.
1. Le premier point repose sur le résultat suivant. Soient X et Y deux matrices $p \times q$. S'il existe $P \in \mathrm{GL}_p(A)$ et $Q \in \mathrm{GL}_q(A)$ telles que $Y = PXQ$, alors, pour $1 \leq k \leq \min\{p, q\}$, l'idéal de A engendré par les mineurs $k \times k$ de X coïncide avec l'idéal de A engendré par les mineurs $k \times k$ de Y.

Une fois ce point acquis, pour démontrer le résultat souhaité, il suffit de montrer que, dans les notations de la proposition, et pour $1 \leq k \leq \min\{p, q\}$, l'idéal engendré par les mineurs $k \times k$ de la matrice

$$\begin{pmatrix} a_1 & 0 & \dots & \dots & 0 & 0 & & 0 \\ 0 & a_2 & 0 & & \vdots & \vdots & & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & a_r & 0 & \dots & 0 \\ 0 & \dots & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

est $\langle a_1 \dots a_k\rangle$ si $k \leq r$ et est nul si $k > r$, ce qui est facile.
2. Le second point se déduit facilement du premier. ∎

Remarque 4.1.5 – **Facteurs invariants** – On suppose A euclidien. Soient $p, q \in \mathbb{N}^*$ des entiers et X une matrice $p \times q$ à coefficients dans A, non nulle et de rang r comme matrice à coefficients dans $\mathbb{K}$. On sait d'après la Proposition 4.1.3 et la Proposition 4.1.4 qu'il existe des matrices $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$ et des éléments $a_1, \ldots, a_r$ non nuls de A vérifiant $a_1 A \supseteq \ldots \supseteq a_r A$ tels que PXQ soit la matrice $(a_{ij})_{1 \le i \le p, 1 \le j \le q}$ où, $a_{ii} = a_i$ pour $1 \le i \le r$ et $a_{ij} = 0$ sinon et que, à multiplication près par des inversibles, les a_i ainsi déterminés sont uniques. Ces éléments sont appelés les *facteurs invariants* de X. (Attention, il y a une ambiguïté dans ce vocabulaire : les facteurs invariants ne sont définis qu'à multiplication près par un inversible.)

Remarque 4.1.6 – Soient $p, q \in \mathbb{N}^*$ des entiers. On rappelle que deux matrices X et Y de $M_{p,q}(A)$ sont dites *équivalentes* s'il existe $P \in \mathrm{GL}_p(A)$ et $Q \in \mathrm{GL}_q(A)$ telles que $Y = PXQ$.

Il est clair alors, si A est euclidien, que deux matrices de $M_{p,q}(A)$ sont équivalentes si et seulement si elles ont les mêmes facteurs invariants.

Exemple 4.1.7 – **Facteurs invariants et matrices compagnons** – Dans cet exemple, on prend $A = \Bbbk[X]$. L'objet est de calculer les facteurs invariants de la matrice $C_P - XI_n$, où $n \in \mathbb{N}^*$, $P = X^n - \sum_{0 \le i \le n-1} a_i X^i \in \Bbbk[X]$ et où C_P est la matrice compagnon de P. On a donc

$$C_P - XI_n = \begin{pmatrix} -X & 0 & 0 & \ldots & 0 & a_0 \\ 1 & -X & 0 & \ldots & 0 & a_1 \\ 0 & 1 & -X & \ldots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} - X \end{pmatrix}.$$

Suivre l'algorithme présenté plus haut n'est pas, dans le cas présent, l'approche la plus rapide. On va procéder de façon plus directe, en effectuant toujours des opérations élémentaires sur les lignes et les colonnes de la matrice considérée afin d'obtenir à chaque étape une matrice équivalent à celle de l'étape précédente.
1. On remplace L_1 par $L_1 + XL_2 + \ldots + X^{n-1} L_n$ et on obtient la matrice équivalente

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -P \\ 1 & -X & 0 & \ldots & 0 & a_1 \\ 0 & 1 & -X & \ldots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} - X \end{pmatrix}.$$

2. On remplace C_2 par $C_2 + XC_1$ puis, dans la matrice obtenu, on remplace C_3 par $C_3 + XC_2$, ..., et enfin $C_n + XC_{n-1}$. On obtient la matrice équivalente :

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -P \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix}.$$

3. On remplace C_n par $C_n - a_1C_1 - \ldots - a_{n-1}C_{n-1}$. On obtient la matrice équivalente :

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -P \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

4. On permute les lignes de manière adéquate pour obtenir la matrice équivalente :

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & -P \end{pmatrix}.$$

Ce qui précède montre que les facteurs invariants de $C_P - XI_n$ sont $1, \ldots, 1, P$.

4.2 Application au calcul effectif des invariants de similitude.

Dans cette section, on met en évidence un moyen effectif de calcul des invariants de similitude d'un endomorphisme en exploitant l'algorithme de calcul des facteurs invariants d'une matrice à coefficients dans $\Bbbk[X]$.

Remarque 4.2.1 – **Calcul effectif des invariants de similitude.** On reprend les notations de la Remarque 3.7. Soit $\mathcal{B}$ une base quelconque de E et M la matrice de f dans la base $\mathcal{B}$. Soit en outre $\mathcal{C}$ une base de E relativement à laquelle la matrice de f est diagonale par bloc et dont les blocs successifs sont les matrices compagnon $C_{P_1}, \ldots, C_{P_r}$ et soit N la matrice de f dans la base $\mathcal{C}$.
1. En utilisant la Remarque 4.1.7, on obtient que, pour $1 \leq i \leq r$, la matrice $C_{P_i} - XI_{\dim(E_i)}$ admet P_i pour seul facteur invariant non inversible. Il s'ensuit facilement que les polynômes $P_1, \ldots, P_r$ sont les facteurs invariants non inversibles de $N - XI_n$.
2. Mais, bien sûr, M et N sont des matrices semblables dans $M_n(\Bbbk)$ et donc $M - XI_n$ et $N - XI_n$ sont semblables dans $M_n(\Bbbk[X])$. Il s'ensuit qu'elles ont les mêmes facteurs invariants.
3. Ce qui précède montre que les polynômes $P_1, \ldots, P_r$ qui interviennent dans la décomposition de Frobenius sont exactement les facteurs invariants non inversibles de la matrice $M - XI_n$, où M est la matrice représentative de f dans une base arbitraire. Il faut cependant prendre garde à l'ordre dans lequel ces polynômes doivent être pris. Plus précisément, puisque la convention du Théorème 3.5 est que $P_r|\ldots|P_1$, les facteurs invariants de $M - XI_n$, dans les conventions de Section 4.1, sont $1, \ldots, 1, P_r, P_2, \ldots, P_1$ (avec $n - r$ occurences de 1).
4. Comme le calcul des facteurs invariants d'une matrice à coefficients dans un anneau euclidien peut se faire par le procédé effectif décrit à la Section 4.1, ce qui précède fournit un moyen effectif de calcul des invariants de similitude d'un endomorphisme.

5 *Exercices.*

Exercice 5.1 – On suppose que E est de dimension finie. Montrer, à l'aide de la Proposition 1.11, que le degré du polynôme minimal de f est majoré par la dimension de E. (Faire le lien avec la Remarque 2.7).

Exercice 5.2 – Soit $n \in \mathbb{N}^*$ et $a_0, \ldots, a_{n-1}$ des éléments de $\mathbb{k}$. Montrer que le déterminant de la matrice

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \vdots & & \ddots & & \vdots & \vdots \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix} - XI_n$$

de $M_n(\mathbb{k}[X])$ est égal à

$$X^n - \sum_{0 \leq i \leq n-1} a_i X^i.$$

Exercice 5.3 – **Démonstration du théorème de Cayley-Hamilton par le calcul matriciel.** Le but de cet exercice est de redémontrer le théorème de Cayley-Hamilton par une méthode plus élémentaire.

Soient $n \in \mathbb{N}^*$ et $M \in M_n(\mathbb{k})$. On pose $\chi_M = \det(M - XI_n)$.

1. Montrer qu'il existe $a_0, \ldots, a_n \in \mathbb{k}$ tels que

$$\chi_M = \sum_{0 \leq i \leq n} a_i X^i.$$

2. Montrer qu'il existe $M_0, \ldots, M_{n-1} \in M_n(\mathbb{k})$ telles que

$${}^t\mathrm{Com}(M - XI_n) = \sum_{0 \leq i \leq n-1} M_i X^i.$$

3. Montrer que

$$\det(M - XI_n) = MM_0 + \sum_{1 \leq i \leq n-1} (MM_i - M_{i-1})\, X^i - M_{n-1} X^n.$$

4. Conclure.

Exercice 5.4 – Calculer les facteurs invariants des matrices à coefficients dans $\mathbb{Z}$ suivantes :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} ; \quad \begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} ; \quad \begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}.$$

Exercice 5.5 – On considère l'endomorphisme f de $\mathbb{R}^4$ dont la matrice représentative dans la base canonique est :

$$\begin{pmatrix} 17 & -8 & -12 & 14 \\ 46 & -22 & -35 & 41 \\ -2 & 1 & 4 & -4 \\ 4 & -2 & -2 & 3 \end{pmatrix}.$$

Calculer les invariants de similitude de f, son polynôme minimal et son polynôme caractéristique et préciser sa réduction de Frobenius.

Chapitre 3

Réduction des endomorphismes.

Dans ce chapitre, E est un espace vectoriel sur $\Bbbk$ et f un endomorphisme de E. On suppose en outre que E est non nul.

1 Sous-espaces propres, diagonalisation.

Définition 1.1 – *Soit* $\lambda \in \Bbbk$.
1. L'espace propre de valeur propre λ *est le sous-espace vectoriel* $\ker(f - \lambda \mathrm{id}_E)$.
2. On dit que λ *est une valeur propre de* f *si* $\ker(f - \lambda \mathrm{id}_E) \neq \{0\}$.
3. Un vecteur propre de valeur propre λ *est un élément non nul* $\ker(f - \lambda \mathrm{id}_E)$.
4. La multiplicité géométrique de λ *est la dimension de* $\ker(f - \lambda \mathrm{id}_E)$.

Définition 1.2 – *On appelle spectre de* f *l'ensemble, noté* $\mathrm{Spec}(f)$*, des valeurs propres de* f.

Lemme 1.3 –
1. Soit $\ell \in \mathbb{N}^*$ *et soient* $\lambda_1, \ldots, \lambda_\ell$ *des valeurs propres deux à deux distinctes de* f*. Alors, les sous-espaces propres* $\ker(f - \lambda_i \mathrm{id}_E)$, $1 \leq i \leq \ell$, *sont en somme directe.*
2. Soit I *un ensemble non vide et* $(\lambda_i)_{i \in I}$ *une famille de valeurs propres de* f *deux à deux distinctes. Alors, les sous-espaces propres* $\ker(f - \lambda_i \mathrm{id}_E)$, $i \in I$, *sont en somme directe.*

Démonstration. Exercice. (Noter que, par définition de la somme directe, le second point se déduit immédiatement du premier.) ∎

Remarque 1.4 – Il découle du Lemme 1.3 que, si E est de dimension finie, alors $\mathrm{Spec}(f)$ est un ensemble fini.

Proposition 1.5 – *Soit* $\lambda \in \Bbbk$*. Les assertions suivantes sont équivalentes :*
(i) $\lambda \in \mathrm{Spec}(f)$ *;*
(ii) λ *est racine de tout polynôme annulateur non nul de* f.

Démonstration. Supposons que $\lambda \in \mathrm{Spec}(f)$ et que $x \in \ker(f - \lambda \mathrm{id}_E)$. Il est facile de montrer que, $P(f)(x) = P(\lambda)x$. On en déduit facilement que la première assertion implique la seconde.

On montre maintenant que $(ii) \Longrightarrow (i)$. Si f n'admet pas de polynôme annulateur non nul, l'implication est triviale. Sinon, le noyau de ev_f est un idéal non nul, et il existe un unique polynôme unitaire μ tel que $\ker(\mathrm{ev}_f) = \langle \mu \rangle$. L'assertion (ii) revient alors à dire que λ est racine de μ. Ainsi, il existe $Q \in \Bbbk[X]$ tel que $\mu = (X - \lambda)Q$. On a donc

$$0 = \mu(f) = (f - \lambda \mathrm{id}_E)Q(f).$$

Mais, par définition de μ, Q n'est pas annulateur de f. Ainsi, il existe $x \in E$ tel que $Q(f)(x) \neq 0$. Mais, d'après l'identité ci-dessus,

$$0 = (f - \lambda \mathrm{id}_E)(Q(f)(x)).$$

Ainsi, $\lambda \in \mathrm{Spec}(f)$. ∎

Proposition 1.6 – *On suppose E de dimension finie. Soit $\lambda \in \Bbbk$. Les assertions suivantes sont équivalentes :*
(i) $\lambda \in \mathrm{Spec}(f)$;
(ii) λ est racine du polynôme caractéristique de f.

Démonstration. Soit $\lambda \in \Bbbk$. On a $\chi_f(\lambda) = \det(f - \lambda \mathrm{id}_E)$. Le reste est clair. ∎

Remarque 1.7 – On suppose E de dimension finie. On a alors l'équivalence des assertions suivantes :
(i) $\lambda \in \mathrm{Spec}(f)$;
(ii) λ est racine du polynôme minimal de f ;
(iii) λ est racine du polynôme caractéristique de f.
Cette équivalence se déduit des Propositions 1.5 et 1.6. On peut aussi la démontrer en remarquant d'abord que, d'après la Remarque 3.8 du Chapitre 2, les racines du polynôme minimal de f et les racines du polynôme caractéristique de f sont les mêmes. L'équivalence ci-dessus se déduit alors de la Proposition 1.5.

Remarque 1.8 – On suppose E de dimension finie. Soit $\lambda \in \mathrm{Spec}(f)$. La multiplicité géométrique de λ est majorée par sa multiplicité comme racine du polynôme caractéristique de f. (Considérer une base de l'espace propre de valeur propre λ, la compléter en une base de E et calculer le polynôme caractéristique de f par le biais de la matrice de f dans la base ainsi obtenue.)

Définition 1.9 – *On dit que f est diagonalisable s'il existe une base de E formée de vecteurs propres de f.*

Remarque 1.10 – Il est clair que les assertions suivantes sont équivalentes :
(i) f est diagonalisable ;
(ii) E est somme directe de sous-espaces de E stables par f et de dimension 1.

Proposition 1.11 –
1. Les assertions suivantes sont équivalentes :
(i) f est diagonalisable :
(ii) on a

$$\bigoplus_{\lambda \in \mathrm{Spec}(f)} \ker(f - \lambda \mathrm{id}_E) = E\,;$$

2. Si E est de dimension finie, les assertions (i) et (ii) ci-dessus sont équivalentes à l'assertion :
(iii) il existe une base relativement à laquelle la matrice de f est diagonale.

Démonstration. Exercice. ∎

Théorème 1.12 – ***Critère de diagonalisabilité via le polynôme caractéristique.*** *On suppose que E est de dimension finie et on note χ_f le polynôme caractéristique de f. Les assertions suivantes sont équivalentes :*
1. f est diagonalisable ;
2. χ_f est scindé et, pour tout $\lambda \in \mathrm{Spec}(f)$, la multiplicité géométrique de λ est égale à sa multiplicité comme racine de χ_f.

Démonstration. Pour tout $\lambda \in \mathrm{Spec}(f)$, on note $m(\lambda)$ la multiplicité géométrique de λ et $m_{\chi_f}(\lambda)$ la multiplicité de λ comme racine de χ_f. D'après la Remarque 1.8,

$$\forall\, \lambda \in \mathrm{Spec}(f), \quad m(\lambda) \leq m_{\chi_f}(\lambda). \tag{3.1}$$

Ainsi, on a :

$$\sum_{\lambda \in \mathrm{Spec}(f)} m(\lambda) \leq \sum_{\lambda \in \mathrm{Spec}(f)} m_{\chi_f}(\lambda) \leq \deg(\chi_f) = \dim(E).$$

De plus, compte tenu de (3.1), la première inégalité est une égalité si et seulement si pour tout $\lambda \in \mathrm{Spec}(f)$, la multiplicité géométrique de λ est égale à sa multiplicité comme racine de χ_f et, compte tenu de la Proposition 1.6, la seconde inégalité est une égalité si et seulement si χ_f est scindé.

L'équivalence de l'énoncé s'ensuit immédiatement d'après le premier point de la Proposition 1.11. ∎

Remarque 1.13 – On suppose que E est de dimension finie. Il découle du Théorème 1.12 que si le polynôme caractéristique de f est scindé et n'a que des racines simples, alors f est diagonalisable.

Théorème 1.14 – ***Critère de diagonalisabilité via le polynôme minimal.*** *On suppose que E est de dimension finie et on note μ_f le polynôme minimal de f. Les assertions suivantes sont équivalentes :*
1. f est diagonalisable ;
2. μ_f est scindé et n'a que des racines simples ;
3. il existe un polynôme annulateur de f scindé et n'ayant que des racines simples.

Démonstration. Il est clair que les assertions 2 et 3 sont équivalentes.

Supposons f diagonalisable. Il existe alors $m \in \mathbb{N}^*$ et $\lambda_1, \ldots, \lambda_m \in \Bbbk$, deux à deux distincts, tels que $\mathrm{Spec}(f) = \{\lambda_1, \ldots, \lambda_m\}$. Une vérification simple montre que le polynôme

$$\prod_{1 \leq i \leq m} (X - \lambda_i)$$

est annulateur de f. Ainsi, la première assertions entraîne les deux autres.

Enfin, supposons que μ_f est scindé et à racines simples. Le Lemme des noyaux appliqué à la décomposition de μ_f en produit d'irréductibles montre que E est somme de ses sous-espaces propres. ■

Remarque 1.15 – Il découle immédiatement de la Remarque 2.5 du Chapitre 1 et du Théorème 1.14 que la restriction à un sous-espace stable d'un endomorphisme diagonalisable est encore diagonalisable.

2 Sous-espaces caractéristiques, décomposition de Dunford.

Dans cette section, on suppose que E est de dimension finie.

De plus, on note μ_f le polynôme minimal de f et χ_f son polynôme caractéristique. Enfin, pour $\lambda \in \mathrm{Spec}(f)$, on note respectivement $m(\lambda)$, $m_{\mu_f}(\lambda)$ et $m_{\chi_f}(\lambda)$ la multiplicité géométrique de λ, sa multiplicité dans le polynôme minimal de f et sa multiplicité dans le polynôme caractéristique de f.

Remarque 2.1 – Soit $\lambda \in \mathrm{Spec}(f)$.
1. On a déjà vu que $1 \leq m(\lambda) \leq m_{\chi_f}(\lambda)$.
2. Il découle du Théorème de Cayley-Hamilton et de la Proposition 1.5 que $1 \leq m_{\mu_f}(\lambda) \leq m_{\chi_f}(\lambda)$.
3. On ne peut pas espérer de résultat général de comparaison entre $m(\lambda)$ et $m_{\mu_f}(\lambda)$ comme le montrent les exemples suivants.
3.1. On considère l'endomorphisme de $\Bbbk^4$ dont la matrice dans la base canonique est

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Un calcul simple montre que $\mathrm{Spec}(f) = \{0\}$ et que $m(0) = 3$, $m_{\mu_f}(0) = 2$, $m_{\chi_f}(0) = 4$. On a donc

$$m_{\mu_f}(0) < m(0) < m_{\chi_f}(0).$$

3.2. On considère l'endomorphisme de $\Bbbk^5$ dont la matrice dans la base canonique est

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Un calcul simple montre que $\mathrm{Spec}(f) = \{0\}$ et que $m(0) = 2$, $m_{\mu_f}(0) = 3$, $m_{\chi_f}(0) = 5$. On a donc

$$m(0) < m_{\mu_f}(0) < m_{\chi_f}(0).$$

Lemme 2.2 – *Soit* $\lambda \in \mathrm{Spec}(f)$. *On a*

$$(0) \subset \ker\left((f-\lambda \mathrm{id}_f)\right) \subseteq \ker\left((f-\lambda \mathrm{id}_f)^{m_{\mu_f}(\lambda)}\right) = \ker\left((f-\lambda \mathrm{id}_f)^{m_{\chi_f}(\lambda)}\right).$$

Démonstration. Soit $\lambda \in \mathrm{Spec}(f)$. On a bien sûr (cf. Remarque 2.1) :

$$(0) \subset \ker\left((f-\lambda \mathrm{id}_f)\right) \subseteq \ker\left((f-\lambda \mathrm{id}_f)^{m_{\mu_f}(\lambda)}\right) \subseteq \ker\left((f-\lambda \mathrm{id}_f)^{m_{\chi_f}(\lambda)}\right).$$

Par ailleurs, le polynôme $X-\lambda$ est un des facteurs irréductible χ_f et de μ_f (cf. Remarque 1.7). La Remarque 2.8 du Chapitre 2 assure alors que la dernière inclusion est une égalité. ■

Définition 2.3 – *Soit* $\lambda \in \mathrm{Spec}(f)$. *On appelle sous-espace caractéristique associé à la valeur propre* λ *le sous-espace vectoriel*

$$\ker\left((f-\lambda \mathrm{id}_f)^{m_{\mu_f}(\lambda)}\right) = \ker\left((f-\lambda \mathrm{id}_f)^{m_{\chi_f}(\lambda)}\right)$$

de E *(cf. Lemme 2.2).*

Remarque 2.4 – Si χ_f est scindé, le Lemme de noyaux et le Théorème de Cayley-Hamilton assurent que E est somme directe de ses sous-espaces caractéristiques.

Proposition 2.5 – **Dimension des sous-espaces caractéristiques** – *Soit* $\lambda \in \mathrm{Spec}(f)$. *On a*

$$\dim\left(\ker\left((f-\lambda \mathrm{id}_f)^{m_{\chi_f}(\lambda)}\right)\right) = m_{\chi_f}(\lambda).$$

Démonstration. On pose $G = \ker\left((f-\lambda \mathrm{id}_f)^{m_{\chi_f}(\lambda)}\right)$; c'est un sous-espace de E stable par f. D'après le Lemme des noyaux et le Théorème de Cayley-Hamilton, il existe un sous-espace H de E, stable par f et supplémentaire de G :

$$E = G \bigoplus H.$$

Notons g l'endomorphisme de G induit par f et h l'endomorphisme de H induit par f.

L'endomorphisme $g-\lambda \mathrm{id}_G$ est un endomorphisme nilpotent de G. Il existe donc une base de G relativement à laquelle la matrice de cet endomorphisme est triangulaire supérieure strice (cf. Exercice 4.4, Chap. 1). La matrice de g dans la base ci-dessus est donc triangulaire supérieure, avec des coefficients diagonaux tous égaux à λ. Si l'on complète cette base en une base de E adaptée à la décomposition $E = G \oplus H$, on obtient l'identité

$$\chi_f = (X-\lambda)^{\dim(G)}\chi_h.$$

De plus, $\chi_h(\lambda) \neq 0$. En effet, dans le cas contraire, il existerait un vecteur propre de valeur propre λ de h et, donc, un vecteur propre de valeur propre λ de f dans H. Ce qui est impossible puisque $\ker(f-\lambda_{\mathrm{id}_E}) \subseteq G$.

On a donc le résultat souhaité. ■

Théorème 2.6 – ***Décomposition de Dunford.*** *On suppose que le polynôme minimal* μ_f *de* f *est scindé. Alors, il existe un unique couple* (d, n) *d'endomorphismes de* E *vérifiant les conditions suivantes :*
1. $f = d + n$,
2. d *et* n *commutent,*
3. d *est diagonalisable,*
4. n *est nilpotent.*
De plus, d *et* n *sont des polynômes de l'endomorphisme* f.

Démonstration. Par hypothèse, il existe $m \in \mathbb{N}^*$, $\lambda_1, \ldots, \lambda_m \in \mathbb{k}$, deux à deux distincts et $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^*$ tels que

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

On a donc $\mathrm{Spec}(f) = \{\lambda_1, \ldots, \lambda_m\}$. Pour $1 \leq i \leq m$, on note E_i le sous-espace caractéristique de f associé à la valeur propre λ_i :

$$E_i = \ker\left((f-\lambda_i \mathrm{id}_E)^{\alpha_i}\right).$$

D'après le Lemme des noyaux, on a donc

$$E = \bigoplus_{1 \leq i \leq m} E_i. \tag{3.2}$$

Pour $1 \leq i \leq m$, on note p_i la projection sur E_i, parallèlement à $\bigoplus_{1 \leq j \leq m,\, j \neq i} E_j$. Enfin, on pose

$$d = \sum_{1 \leq i \leq m} \lambda_i p_i \qquad \text{et} \qquad n = f - d.$$

On rappelle que, d'après le Lemme des noyaux, pour $1 \leq i \leq m$, p_i est un polynôme en f. Il s'ensuit que d et n sont des polynômes en f. En particulier, ils commutent entre eux.

Précisons davantage la description de d et n. On note pour commencer que, étant des polynôme en f, d et n laissent stables les sous-espaces caractéristiques E_i, $1 \leq i \leq n$. En outre, par définition de d, si $1 \leq i \leq m$ et si $x \in E_i$, on a $d(x) = x$. Ainsi, $d_{|E_i} = \lambda_i \mathrm{id}_{E_i}$. Il s'ensuit que d est diagonalisable et que la décomposition (3.2) est sa décomposition en sous-espaces propres. Enfin, soit $1 \leq i \leq m$. Comme f, d et n stabilisent E_i, on a

$$n_{|E_i} = f_{|E_i} - d_{|E_i} = f_{|E_i} - \lambda_i \mathrm{id}_{E_i},$$

ce dont il découle que $(n_{|E_i})^{\alpha_i} = 0$, par définition de E_i. La restriction de n à E_i est donc nilpotente. Par suite, pour $1 \leq i \leq m$, les endomorphismes

$$E \xrightarrow{p_i} E_i \xrightarrow{n_{|E_i}} E_i \xrightarrow{inj.can.} E$$

sont nilpotents et commutent deux à deux. Comme n est leur somme, n est nilpotent. Le couple (d, n) ainsi construit vérifie donc les conditions requises.

Supposons que $(\tilde{d}, \tilde{n})$ soit un autre couple qui les satisfait. Comme $\tilde{d}$ et $\tilde{n}$ commutent, ils commutent avec leur somme f. Et, comme d et n sont des polynômes en f, $\tilde{d}$ et $\tilde{n}$ commutent avec chacun d'eux. Cela montre que $n - \tilde{n}$ est nilpotent (utiliser la formule du binôme) et que $d - \tilde{d}$ est diagonalisable (utiliser la diagonalisation simultanée des endomorphismes diagonalisables qui commutent). Mais alors, l'endomorphisme

$$n - \tilde{n} = -(d - \tilde{d})$$

est nilpotent et diagonalisable, ce qui assure qu'il est nul. L'unicité s'ensuit. ∎

3 Décomposition de Jordan.

Dans cette section, on suppose que E est de dimension finie.

Définition 3.1 – *Soit $d \in \mathbb{N}^*$. On appelle matrice de Jordan (ou bloc de Jordan) de taille d la matrice $J_d \in M_d(\mathbb{k})$ dont les coefficients sont tous nuls, sauf ceux situés sur la ligne i et la colonne $i+1$, $1 \leq i \leq d-1$, qui valent* 1.

Remarque 3.2 – On suppose qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E telle que la matrice représentative de f dans la base $\mathcal{B}$ soit J_n.
1.1. Il est facile de voir que f est nilpotent d'indice n.
1.2. Plus précisément, pour $0 \leq k \leq n-1$,

$$\mathrm{Im}\left(f^k\right) = \mathrm{Vect}\{e_1, \ldots, e_{n-k}\}.$$

Remarque 3.3 – On suppose qu'il existe $r \in \mathbb{N}^*$, une suite décroissante $d_1 \geq d_2 \geq \ldots \geq d_r$ d'éléments de $\mathbb{N}^*$ et une base $\mathcal{B}$ de E tels que la matrice représentative de f dans la base $\mathcal{B}$ soit diagonale par blocs, les blocs diagonaux étant les blocs de Jordan $J_{d_1}, \ldots, J_{d_r}$. On a donc $\dim(E) = d_1 + \ldots + d_r$.
1. Il est facile de voir que f est nilpotent d'indice d_1, que son noyau est de dimension r et que son rang est $d_1 + \ldots + d_r - r$.

2. Posons $E_1 = \mathrm{Vect}\{e_1, \ldots, e_{d_1}\}$ et, pour $2 \leq i \leq r$, $E_i = \mathrm{Vect}\{e_{d_1+\ldots+d_{i-1}+1}, \ldots, e_{d_1+\ldots+d_i}\}$. Alors, les sous-espaces $E_1, \ldots, E_r$ sont stables par f et

$$E = \bigoplus_{1 \leq i \leq r} E_i.$$

Notons f_i l'endomorphisme de E_i induit par f, $1 \leq i \leq r$. Soit $k \in \mathbb{N}$. On a donc que

$$\mathrm{rg}\left(f^k\right) = \sum_{1 \leq i \leq r} \mathrm{rg}\left(f_i^k\right).$$

Introduisons la notation suivante : si $p \in \mathbb{Z}$, on pose $p_+ = p$ si $p \geq 0$ et $p_+ = 0$ si $p < 0$. Avec ce qui précède et la Remarque 3.2, on obtient que

$$\mathrm{rg}\left(f^k\right) = \sum_{1 \leq i \leq r} (d_i - k)_+.$$

Il s'ensuit que, pour tout $k \in \mathbb{N}^*$,

$$\begin{aligned}
\mathrm{rg}(f^{k+1}) + \mathrm{rg}(f^{k-1}) - 2\mathrm{rg}(f^k) &= \sum_{1 \leq i \leq r} ((d_i - k - 1)_+ + (d_i - k + 1)_+ - 2(d_i - k)_+) \\
&= \sum_{1 \leq i \leq r, d_i = k} ((d_i - k - 1)_+ + (d_i - k + 1)_+ - 2(d_i - k)_+) \\
&= \sum_{1 \leq i \leq r, d_i = k} 1 \\
&= |\{i \in \mathbb{N}, | \, 1 \leq i \leq r, \, d_i = k\}|.
\end{aligned}$$

On a donc montré que le nombre d'occurences de $k \in \mathbb{N}^*$ dans la suite finie $d_1 \geq \ldots \geq d_r$ est $\mathrm{rg}(f^{k+1}) + \mathrm{rg}(f^{k-1}) - 2\mathrm{rg}(f^k)$.

On déduit de cela que la suite $d_1 \geq \ldots \geq d_r$ est indépendante de $\mathcal{B}$.

Théorème 3.4 – ***Réduction de Jordan, cas nilpotent.*** *On suppose f nilpotent. Alors, il existe $r \in \mathbb{N}^*$, une suite décroissante $d_1 \geq d_2 \geq \ldots \geq d_r$ d'éléments de $\mathbb{N}^*$ et une base $\mathcal{B}$ de E tels que la matrice représentative de f dans la base $\mathcal{B}$ soit diagonale par blocs, les blocs diagonaux étant les blocs de Jordan $J_{d_1}, \ldots, J_{d_r}$.*

Démonstration. On procède par récurrence sur la dimension de l'espace E. Si E est de dimension 1, f est nul et le résultat est immédiat. Soit $n \in \mathbb{N}^*$. Supposons le résultat vrai pour tout espace de dimension n et supposons que E est de dimension $n + 1$. Les Propositions 3.3 et 1.11 du Chapitre 2 assurent qu'il existe un élément non nul $x \in E$ tel que le sous-espace cyclique $E_{f,x}$ ait un supplémentaire stable par f et $\mu_f = \mu_{f,x}$. Soient x un tel élément et F un tel supplémentaire. On a :

$$E = E_{f,x} \bigoplus F.$$

L'hypothèse de récurrence appliquée à la restriction de f à F fournit une base de F relativement à laquelle la matrice de cette restriction est diagonale par blocs, les blocs diagonaux étant les blocs de Jordan $J_{d_2} \ldots, J_{d_r}$, où $d_2 \geq \ldots \geq d_r$ sont des entiers strictement positifs.

Par ailleurs, posons $d_1 = \deg(\mu_f)$. En particulier, d_1 est l'indice de nilpotence de f. La Proposition 1.9 du Chapitre 2 assure que $(f^{d_1-1}(x), \ldots, f(x), x)$ est une base de $E_{f,x}$ et il est clair que la matrice de la restriction de f à $E_{f,x}$ dans cette base est un bloc de Jordan de taille d_1. Comme μ_f annule la restriction de f à F et comme d_2 est le degré du polynôme minimal de cette restriction, on a bien $d_1 \geq d_2$. La base obtenue en complétant $(f^{d_1-1}(x), \ldots, f(x), x)$ par la base de F mentionnée plus haut donne le résultat. ■

Théorème 3.5 – ***Réduction de Jordan.*** *On suppose que le polynôme minimal μ_f de f est scindé et on pose* $\mathrm{Spec}(f) = \{\lambda_1, \ldots, \lambda_m\} \subseteq \Bbbk$ *($m \in \mathbb{N}^*$). Alors, il existe $r_1, \ldots, r_m \in \mathbb{N}^*$ et m suites finies décroissantes $d_{i,1} \geq \ldots \geq d_{i,r_i}$, $1 \leq i \leq m$, d'éléments de $\mathbb{N}^*$ et une base $\mathcal{B}$ de E tels que la matrice représentative de f dans la base $\mathcal{B}$ soit diagonale par blocs, les blocs diagonaux étant*

$$\lambda_i I_{d_{i,j}} + J_{d_{i,j}}, \quad 1 \leq i \leq m, \quad 1 \leq j \leq r_i.$$

Démonstration. On reprend, en la raffinant, la démonstration du Théorème 2.6. Par hypothèse, il existe $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^*$ tels que

$$\mu_f = \prod_{1\leq j\leq m} (X-\lambda_j)^{\alpha_i}.$$

Pour $1 \leq i \leq m$, on note E_i le sous-espace caractéristique de f associé à la valeur propre λ_i :

$$E_i = \ker\left((f-\lambda_i \mathrm{id}_E)^{\alpha_i}\right).$$

D'après le Lemme des noyaux, on a :

$$E = \bigoplus_{1\leq i\leq m} E_i.$$

Soit $1 \leq i \leq m$. La restriction à E_i de $f - \lambda_i \mathrm{id}_E$ est un endomorphisme nilpotent. Donc, d'après le Théorème 3.4, il existe un entier $r_i \in \mathbb{N}^*$, une suite $d_{i,1} \geq \ldots \geq d_{i,r_i}$ d'éléments de $\mathbb{N}^*$ et une base $\mathcal{B}_i$ de E_i tels que la matrice de la restriction en question, relativement à la base $\mathcal{B}_i$, soit diagonale par blocs, les blocs étant

$$J_{d_{i,1}}, \ldots, J_{d_{i,r_i}}.$$

Avec ces notations, la matrice relativement à $\mathcal{B}_i$ de la restriction de f à E_i est donc diagonale par blocs, les blocs étant

$$\lambda_i I_{d_{i,1}} + J_{d_{i,1}}, \ldots, \lambda_i I_{d_{i,r_i}} + J_{d_{i,r_i}}.$$

Si $\mathcal{B}$ est la base obtenue en réunissant les bases $\mathcal{B}_i$, $1 \leq i \leq m$, la matrice de f relativement à $\mathcal{B}$ est comme requise par l'énoncé. ∎

La démonstration du Théorème 3.4 met clairement en évidence que l'obtention d'une base explicite relativement à laquelle la matrice de f est sous forme de Jordan se ramène à la détermination d'une telle base lorsque f est nilpotent. On étudie donc maintenant un procédé effectif de détermination d'une base de E relativement à laquelle la matrice de f est sous forme de Jordan dans le cas d'un endomorphisme f nilpotent.

Remarque 3.6 – ***Détermination d'une base de Jordan pour un endomorphisme nilpotent.*** On suppose que f est un endomorphisme nilpotent, d'indice $p \in \mathbb{N}^*$.

On rappelle qu'on a alors une suite strictement croissante de sous-espaces vectoriels comme suit :

$$\{0\} \subset \ker(f) \subset \ker(f^2) \subset \ldots \subset \ker(f^{p-1}) \subset \ker(f^p) = E. \tag{3.3}$$

On rappelle aussi que, pour $1 \leq i \leq p$,

$$f(\ker(f^i)) \subseteq \ker(f^{i-1}).$$

Le procédé consiste à construire, en p étapes, une base particulière de E, adaptée (en un sens à préciser) à la suite (3.3) de sous-espaces et à f.

Etape 0. Soit F_p un supplémentaire de $\ker(f^{p-1})$ dans $\ker(f^p) = E$, soit m_p sa dimension et soit $\mathcal{B}_p = \{e_{1,p}, \ldots, e_{m_p,p}\}$ une base de F_p. En résumé :

$$E = \ker(f^p) = \ker(f^{p-1}) \bigoplus F_p, \qquad F_p = \mathrm{Vect}(\mathcal{B}_p).$$

Etape 1. On observe que la restriction de f à F_p est injective (pour $p \geq 2$) puisque $\ker(f) \cap F_p = \{0\}$. Ainsi, $f(\mathcal{B}_p)$ est une famille libre de $\ker(f^{p-1})$. On vérifie facilement que $\ker(f^{p-2})$ et $f(F_p)$ sont en somme directe et on choisit un supplémentaire G_{p-1} de $\ker(f^{p-2}) \oplus f(F_p)$ dans $\ker(f^{p-1})$. En résumé :

$$\ker(f^{p-1}) = \ker(f^{p-2}) \bigoplus f(F_p) \bigoplus G_{p-1}.$$

Posons $F_{p-1} = f(F_p) \bigoplus G_{p-1}$, $m_{p-1} = \dim(G_{p-1})$ et choisissons une base $\{e_{m_p+1,p-1}, \ldots, e_{m_p+m_{p-1},p-1}\}$ de G_{p-1}. Posons enfin $e_{i,p-1} = f(e_{i,p})$, pour $1 \leq i \leq m_p$ et

$$\mathcal{B}_{p-1} = \{e_{1,p-1}, \ldots, e_{m_p,p-1}, e_{m_p+1,p-1}, \ldots, e_{m_p+m_{p-1},p-1}\}.$$

D'après ce qui précède, $\mathcal{B}_{p-1}$ est une base de F_{p-1} et

$$\ker(f^{p-1}) = \ker(f^{p-2}) \bigoplus F_{p-1}, \qquad F_{p-1} = \mathrm{Vect}(\mathcal{B}_{p-1}).$$

Etape 2. On procède de même en construisant une décomposition

$$\ker(f^{p-2}) = \ker(f^{p-3}) \bigoplus f(F_{p-1}) \bigoplus G_{p-2}.$$

On pose $F_{p-2} = f(F_{p-1}) \bigoplus G_{p-2}$, $m_{p-2} = \dim(G_{p-2})$ et on choisit une base $\{e_{m_p+m_{p-1}+1,p-2}, \ldots, e_{m_p+m_{p-1}+m_{p-2},p-2}\}$ de G_{p-2}. On pose $e_{i,p-2} = f(e_{i,p-1})$, pour $1 \leq i \leq m_p + m_{p-1}$ et

$$\mathcal{B}_{p-2} = \{e_{1,p-2}, \ldots, e_{m_p+m_{p-1}+m_{p-2},p-2}\}.$$

D'après ce qui précède, $\mathcal{B}_{p-2}$ est une base de F_{p-2} et

$$\ker(f^{p-2}) = \ker(f^{p-3}) \bigoplus F_{p-2}, \qquad F_{p-2} = \mathrm{Vect}(\mathcal{B}_{p-2}).$$

On itère ce procédé jusqu'à aboutir à l'étape $p-2$ qui fournit une décomposition :

$$\ker(f^2) = \ker(f) \bigoplus F_2$$

et une base de $\mathcal{B}_2$ de F_2.

Etape p-1. On procède de même en construisant une décomposition

$$\ker(f) = \ker(f^0) \bigoplus f(F_2) \bigoplus G_1.$$

On pose $F_1 = f(F_2) \bigoplus G_1$, $m_1 = \dim(G_1)$ et on choisit une base $\{e_{m_p+\ldots+m_2+1,1}, \ldots, e_{m_p+\ldots+m_2+m_1,1}\}$ de G_1. On pose $e_{i,1} = f(e_{i,2})$, pour $1 \leq i \leq m_p + \ldots + m_2$ et

$$\mathcal{B}_1 = \{e_{1,1}, \ldots, e_{m_p+\ldots+m_1,1}\}.$$

D'après ce qui précède, $\mathcal{B}_1$ est une base de F_1 et

$$\ker(f) = \{0\} \bigoplus F_1, \qquad F_1 = \mathrm{Vect}\{\mathcal{B}_1\}.$$

Bilan. On a ainsi construit des sous-espaces vectoriels $F_1, \ldots, F_p$ de E tels que

$$E = F_1 \bigoplus \ldots \bigoplus F_p$$

et, pour $1 \leq i \leq p$, une base $\mathcal{B}_i$ de F_i. Bien sûr, si l'on pose

$$\mathcal{B} = \cup_{1 \leq i \leq p} \mathcal{B}_i,$$

$\mathcal{B}$ est une base de E.

Revenons sur la construction de $\mathcal{B}$. Les éléments de $\mathcal{B}$ sont les $e_{i,j}$ où le couple (i,j) parcourt le sous-ensemble $\mathcal{E}$ de $\mathbb{N}^2$ suivant

$$\mathcal{E} = \{(i,j) \in \mathbb{N}^2,\ 1 \leq j \leq p,\ 1 \leq i \leq m_p + \ldots + m_j\}.$$

Si l'on ordonne les éléments de $\mathcal{B}$ en suivant l'ordre lexicographique de $\mathcal{E}$, la matrice de f dans $\mathcal{B}$ est clairement sous forme de Jordan.

Remarque 3.7 – On reprend les notations de la Remarque 3.6.
1. Pour $1 \leq i \leq p$, on a un isomorphisme d'espaces vectoriels comme suit :

$$F_i \cong \ker(f^i)/\ker(f^{i-1})$$

2. Pour la cohérence des notations, posons $G_p = F_p$. Pour $1 \leq i \leq p$, on a posé $m_i = \dim(G_i)$, et on a :

$$m_i = \dim(G_i) = 2\dim(\ker(f^i)) - \dim(\ker(f^{i+1})) - \dim(\ker(f^{i-1})). \tag{3.4}$$

Ainsi, d'après la Remarque 3.3, pour $1 \leq i \leq p$, m_i est le nombre de blocs de Jordan de taille i dans la forme réduite de Jordan de f.

Exemple 3.8 – On illustre ce qui précède par un exemple explicite. On considère un endomorphisme f de $\Bbbk^{12}$, nilpotent d'indice 4 et tel que

$$\dim(\ker(f)) = 5, \qquad \dim(\ker(f^2)) = 8, \qquad \dim(\ker(f^3)) = 11, \qquad \dim(\ker(f^4)) = 12.$$

Un calcul immédiat avec (3.4) donne que

$$m_4 = 1, \qquad m_3 = 2, \qquad m_2 = 0, \qquad m_1 = 2.$$

La base construite à la Remarque 3.6 se schématise donc comme suit :

$$\begin{array}{llllll}
\mathcal{B}_4 & e_{1,4} & & & & \\
 & \downarrow & & & & \\
\mathcal{B}_3 & e_{1,3} & e_{2,3} & e_{3,3} & & \\
 & \downarrow & \downarrow & \downarrow & & \\
\mathcal{B}_2 & e_{1,2} & e_{2,2} & e_{3,2} & & \\
 & \downarrow & \downarrow & \downarrow & & \\
\mathcal{B}_1 & e_{1,1} & e_{2,1} & e_{3,1} & e_{4,1} & e_{5,1}
\end{array}$$

On considère donc

$$\mathcal{B} = (e_{1,1}, e_{1,2}, e_{1,3}, e_{1,4}, e_{2,1}, e_{2,2}, e_{2,3}, e_{3,1}, e_{3,2}, e_{3,3}, e_{4,1}, e_{5,1}).$$

La matrice de f dans $\mathcal{B}$ est la suivante :

$$\begin{pmatrix}
0 & 1 & 0 & 0 & & & & & & & & \\
0 & 0 & 1 & 0 & & & & & & & & \\
0 & 0 & 0 & 1 & & & & & & & & \\
0 & 0 & 0 & 0 & & & & & & & & \\
 & & & & 0 & 1 & 0 & & & & & \\
 & & & & 0 & 0 & 1 & & & & & \\
 & & & & 0 & 0 & 0 & & & & & \\
 & & & & & & & 0 & 1 & 0 & & \\
 & & & & & & & 0 & 0 & 1 & & \\
 & & & & & & & 0 & 0 & 0 & & \\
 & & & & & & & & & & 0 & \\
 & & & & & & & & & & & 0
\end{pmatrix}$$

4 *Exercices.*

Exercice 4.1 – On suppose E de dimension finie et on considère un endomorphisme f tel qu'il existe une base de E relativement à laquelle la matrice de f est diagonale par blocs, avec pour blocs $J_{d_1}, \ldots, J_{d_r}$ où $r \in \mathbb{N}^*$, et $d_1 \geq \ldots \geq d_r \in \mathbb{N}$. Calculer les trois multiplicités de l'unique valeur propre 0 de f.

Exercice 4.2 – **Diagonalisation simultanée.** On suppose E de dimension finie. On considère $N \in \mathbb{N}^*$ et une famille $(f_i)_{1\leq i\leq N}$ d'éléments de $\mathrm{End}_{\Bbbk}(E)$. On dit qu'une telle famille est simultanément diagonalisable s'il existe une base de E relativement à laquelle, pour tout entier i tel que $1 \leq i \leq N$, la matrice de f_i est diagonale.

Le but de cet exercice est de montrer l'équivalence des assertions suivantes :
(i) $(f_i)_{1\leq i\leq N}$ est simultanément diagonalisable ;
(ii) les f_i, $1 \leq i \leq N$, sont diagonalisables et commutent deux-à-deux.
1. Montrer que (i) implique (ii).
2. Le but de cette question est de montrer que (ii) implique (i).
2.1. Montrer que si deux endomorphismes de E commutent, alors les sous-espaces propres de l'un sont stables par l'autre.
2.2 Conclure à l'aide d'une récurrence sur N.

Exercice 4.3 – Soit n un entier tel que $n \geq 2$ et soit A la matrice $n \times n$ à coefficients réels dont tous les coefficients en première ou dernière ligne et tous les coefficients en première et dernière colonne valent 1 et dont tous les autre coefficients sont nuls. On considère l'endomorphisme $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ dont la matrice dans la base canonique est A. En calculant la trace de A et de A^2, montrer que f est diagonalisable et diagonaliser f.

Exercice 4.4 – **Trigonalisation.** On suppose E de dimension finie. On rappelle qu'un endomorphisme est dit trigonalisable s'il existe une base de E relativement à laquelle la matrice de f est triangulaire supérieure.

Le but de cet exercice est de montrer l'équivalence des assertions suivantes :
(i) f est trigonalisable ;
(ii) le polynôme caractéristique de f est scindé.
(En fait, la démonstration de ce résultat fournit aussi un moyen pratique de trigonalisation.)
1. Montrer que (i) implique (ii).
2. Soit u un endomorphisme de E dont le polynôme caractéristique, χ_u, est scindé. On propose ci-dessous deux démonstrations de l'implication (ii) $\Rightarrow$ (i).
2.1. Démonstration par les sous-espaces stables.
2.1.1. Montrer que u admet une valeur propre.
2.1.2. Soit λ une valeur propre de u. Montrer que $\mathrm{Im}(u - \lambda \mathrm{id})$ est une sous-espace vectoriel de E de dimension au plus égale à $n-1$.
2.1.3. Montrer qu'il existe un hyperplan H de E tel que $\mathrm{Im}(u - \lambda \mathrm{id}) \subseteq H$. Montrer que pour tout tel hyperplan, on a $u(H) \subseteq H$.
2.1.4. Montrer qu'il existe une base de E relativement à laquelle la matrice de u est de la forme suivante :

$$\begin{pmatrix} a_{11} & \dots & \dots & a_{1,n-1} & a_{1n} \\ \vdots & & & \vdots & \vdots \\ \vdots & & & \vdots & \vdots \\ a_{n-1,1} & \dots & \dots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}.$$

2.1.5. On note v la restriction de u à H. Montrer que le polynôme caractéristique de v est scindé.
2.1.6. Conclure.
2.2. Démonstration par passage au quotient.
2.2.1. Montrer que u admet une valeur propre.
2.2.2. Soit λ une valeur propre de u, x un vecteur propre de valeur propre λ et posons $D = \mathbb{k}.x$.
2.2.3. Montrer que u induit un endomorphisme $\tilde{u}$ de l'espace vectoriel quotient E/D.
2.2.4. Montrer que si $\tilde{u}$ est trigonalisable, alors u l'est aussi.
2.2.5. Conclure.

Exercice 4.5 – Déterminer la décomposition de Dunford de l'endomorphisme f de $\mathbb{C}^3$ dont la matrice relativement à la base canonique est A dans les trois cas suivants :
1. $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$; 2. $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$; 3. $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$.

Exercice 4.6 – Soit f l'endomorphisme de $\mathbb{C}^3$ dont la matrice relativement à la base canonique est $A = \begin{pmatrix} 3 & 0 & 8 \\ 3 & -1 & 6 \\ -2 & 0 & -5 \end{pmatrix}$. Sachant que le polynôme caractéristique de f est $(X+1)^3$, déterminer la décomposition de Dunford de f. En déduire f^n, pour tout $n \in \mathbb{N}$.

Exercice 4.7 – Soient $\lambda, \mu, a, b, c \in \mathbb{C}$ avec $\lambda \neq \mu$. On considère l'endomorphisme f de $\mathbb{C}^3$ dont la matrice dans la base canonique de $\mathbb{C}^3$ est $A = \begin{pmatrix} \lambda & a & b \\ 0 & \mu & c \\ 0 & 0 & \lambda \end{pmatrix}$.

1. Calculer le polynôme caractéristique de f.
2. A quelle condition sur les paramètres f est-il diagonalisable ?
3. Déterminer la réduction de Jordan de f.

Exercice 4.8 – Soit $\Bbbk$ un corps.
1. On considère $u : \Bbbk^{10} \longrightarrow \Bbbk^{10}$ endomorphisme tel que $u^3 = 0$, $\mathrm{rg}(u^2) = 2$ et $\mathrm{rg}(u) = 5$. Ecrire la matrice de la forme normale de Jordan de u.
2. Existe-t-il un endomorphisme $u : \Bbbk^{10} \longrightarrow \Bbbk^{10}$ tel que $u^4 = 0$, $\mathrm{rg}(u^3) = 2$, $\mathrm{rg}(u^2) = 2$ et $\mathrm{rg}(u) = 5$.

Exercice 4.9 – On considère l'endomorphisme u de $\mathbb{C}^4$ dont la matrice dans la base canonique est
$$A = \begin{pmatrix} 0 & 1 & -1 & 0 \\ -3 & -1 & 3 & 1 \\ -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$
1. Calculer et factoriser le polynôme caractéristique de u.
2. Pour $\lambda \in \mathrm{Spec}(u)$, déterminer explicitement la suite $\left(\ker\left((u - \lambda \mathrm{id}_{\mathbb{C}^4})^k\right)\right)_{k\in\mathbb{N}}$ en donnant une base des sous-espaces de cette suite.
3. Déterminer une base de E relativement à laquelle la matrice de u est sous forme réduite de Jordan.

Exercice 4.10 – **Rang et sous-espaces caractéristiques.** On considère un endomorphisme f de l'espace vectoriel E. On suppose en outre qu'il existe un ensemble I non vide et des sous-espaces E_i, $i \in I$, stables par f et tels que
$$E = \bigoplus_{i\in I} E_i.$$
En outre, pour $i \in I$, on note f_i l'endomorphisme de E_i induit par f.
1. Montre que
$$\ker(f) = \bigoplus_{i\in I} \ker(f_i) \qquad \text{et} \qquad \mathrm{Im}(f) = \bigoplus_{i\in I} \mathrm{Im}(f_i)$$
2. On suppose que E est de dimension finie et que le polynôme minimal de f est scindé. Pour $\lambda \in \mathrm{Spec}(f)$, on note E_λ le sous-espace caractéristique de f associé à λ, d_λ sa dimension et f_λ l'endomorphisme induit par f sur E_λ. Montrer la formule suivante :
$$\forall \lambda \in \mathrm{Spec}(f),\ \forall \ell \in \mathbb{N}, \qquad \mathrm{rg}\left((f - \lambda \mathrm{id}_E)^\ell\right) = \mathrm{rg}\left((f_\lambda - \lambda \mathrm{id}_{E_\lambda})^\ell\right) + \sum_{\mu\in\mathrm{Spec}(f),\, \mu\neq\lambda} d_\lambda$$

Exercice 4.11 – **Rappels sur la relation de similitude.** Soit E un espace vectoriel sur $\Bbbk$. On considère dans $\mathrm{End}_\Bbbk(E)$ la relation binaire $\sim$ défini par
$$\forall\, f, g \in \mathrm{End}_\Bbbk(E), \qquad f \sim g \quad \text{si} \quad \exists \sigma \in \mathrm{Aut}_\Bbbk(E) \mid g = \sigma f \sigma^{-1}.$$
Les classes d'équivalence pour cette relation sont appelées *classes de similitude* et deux endomorphismes sont dits *semblables* s'ils sont équivalents.
1. Montrer que la relation $\sim$ est une relation d'équivalence.
2. Soient $f, g \in \mathrm{End}_\Bbbk(E)$ et supposons qu'il existe $\sigma \in \mathrm{Aut}_\Bbbk(E)$ tel que $g = \sigma f \sigma^{-1}$. Montrer que $\ker(g) = \sigma(\ker(f))$ et $\mathrm{Im}(g) = \sigma(\mathrm{Im}(f))$. En déduire que, pour tout $\lambda \in \Bbbk$ et $\ell \in \mathbb{N}$,
$$\ker\left((g - \lambda \mathrm{id}_E)^\ell\right) = \sigma\left(\ker\left((f - \lambda \mathrm{id}_E)^\ell\right)\right) \qquad \text{et} \qquad \mathrm{Im}\left((g - \lambda \mathrm{id}_E)^\ell\right) = \sigma\left(\mathrm{Im}\left((f - \lambda \mathrm{id}_E)^\ell\right)\right).$$
3. Soient $f, g \in \mathrm{End}_\Bbbk(E)$, semblables. Montrer que f est nilpotent si et seulement si g l'est et montrer que si f et g sont nilpotents, ils ont même indice de nilpotence.
4. On suppose E de dimension finie.
4.1. Soient $f, g \in \mathrm{End}_\Bbbk(E)$, semblables. Montrer que, pour tout $\lambda \in \Bbbk$ et $\ell \in \mathbb{N}$,
$$\mathrm{rg}\left((g - \lambda \mathrm{id}_E)^\ell\right) = \mathrm{rg}\left((f - \lambda \mathrm{id}_E)^\ell\right).$$
4.2. Soient $f, g \in \mathrm{End}_\Bbbk(E)$ et $\sigma \in \mathrm{Aut}_\Bbbk(E)$. Montrer que, pour toute base $\mathcal{B}$ de E, $\mathrm{Mat}_\mathcal{B}(g) = \mathrm{Mat}_{\sigma(\mathcal{B})}(f)$.
4.3. Soient $f, g \in \mathrm{End}_\Bbbk(E)$ et $\mathcal{B}$ une base de E. Montrer que f et g sont semblables si et seulement si il existe une base $\mathcal{C}$ de E telle que $\mathrm{Mat}_\mathcal{B}(g) = \mathrm{Mat}_\mathcal{C}(f)$.

Exercice 4.12 – **Réduction de Jordan et classes de similitude.** Le but de cet exercice est de démontrer le résultat suivant : si f et g sont deux endomorphismes d'un espace vectoriel de dimension finie et si les polynômes minimaux de f et g sont scindés, alors f et g sont semblables si et seulement si,

$$\forall \lambda \in \Bbbk, \quad \forall \ell \in \mathbb{N}, \qquad \mathrm{rg}\left((f - \lambda \mathrm{id}_E)^\ell\right) = \mathrm{rg}\left((g - \lambda \mathrm{id}_E)^\ell\right). \tag{3.5}$$

Pour cela, on utilisera les résultats de l'Exercice 4.10 et de l'Exercice 4.11.

Dans la suite, on fixe $f, g \in \mathrm{End}_{\Bbbk}(E)$ et on suppose que f et g ont un polynôme minimal scindé.

1. Montrer que si f et g sont semblables, alors on a les identités (3.5).

2. On suppose dans cette question que f et g satisfont les identités (3.5).

2.1. Montrer que $\mathrm{Spec}(f) = \mathrm{Spec}(g)$. On pose $\mathcal{S} = \mathrm{Spec}(f) = \mathrm{Spec}(g)$.

2.2. Pour $\lambda \in \mathcal{S}$, on note respectivement $E_{f,\lambda}$ et $E_{g,\lambda}$ les sous-espaces caractéristique de f et g associée à la valeur propre λ. Montrer que

$$\forall \lambda \in \mathcal{S}, \qquad \dim(E_{f,\lambda}) = \dim(E_{g,\lambda}).$$

(On pourra considérer les suites de noyaux itérés $\left(\ker\left((f - \lambda \mathrm{id}_E)^\ell\right)\right)_{\ell \in \mathbb{N}}$ et $\left(\ker\left((g - \lambda \mathrm{id}_E)^\ell\right)\right)_{\ell \in \mathbb{N}}$.)

2.3. Pour $\lambda \in \mathcal{S}$, on note respectivement f_λ et g_λ les endomorphismes induits par f et g sur $E_{f,\lambda}$ et $E_{g,\lambda}$. Montrer qu'il existe une base $\mathcal{B}_\lambda$ de $E_{f,\lambda}$ et une base $\mathcal{C}_\lambda$ de $E_{g,\lambda}$ telle que

$$\mathrm{Mat}_{\mathcal{B}_\lambda}(f_\lambda - \lambda \mathrm{id}_{E_{f,\lambda}}) = \mathrm{Mat}_{\mathcal{C}_\lambda}(g_\lambda - \lambda \mathrm{id}_{E_{g,\lambda}}).$$

(On pourra utiliser la réduction de Jordan dans le cas nilpotent.)

2.4. En déduire qu'il existe une base $\mathcal{B}$ et une base $\mathcal{C}$ de E telles que

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

2.5. Conclure que f et g sont semblables. (Cf. Exercice 4.11.)