## 1.6 Sous-espaces cycliques

### 1.6.1 Sous-espaces cycliques d'un endomorphisme

Soit $u \in L(E)$ fixé. On peut munir $E$ d'une structure de $\mathbf{K}[X]$-module (mêmes définitions qu'un espace vectoriel mais le corps est remplacé par un anneau commutatif quelconque, ici $\mathbf{K}[X]$) en prenant pour loi externe :

$$\forall\ P \in \mathbf{K}[X],\ \forall\ y \in E\ :\ P.y\ =\ P(u)(y).$$

On note $E_u$ ce $\mathbf{K}[X]$-module. Si $F$ est un sous-module de $E_u$ alors c'est aussi un sous-espace vectoriel de $E$ et pour tout $y$ de $F$ on a $X.y \in F$ i.e $u(y) \in F$ donc $F$ est un sous-espace vectoriel de $E$ stable par $u$; la réciproque est évidente donc <u>*les sous-modules de $E_u$ sont les sous-espaces vectoriels de E stables par u*</u>.

Si $x$ est un élément de $E$ on note $E_x$ le sous-module engendré par $x$ (i.e le plus petit sous-module de $E_u$ contenant $x$). On voit immédiatement que c'est l'ensemble $\{P.x = P(u)(x) / P \in \mathbf{K}[X]\}$qui est aussi le plus petit sous-espace vectoriel de $E$ stable par $u$. On l'appelle <u>*sous-espace cyclique*</u> engendré par $x$.

On dit que $E$ est <u>*cyclique*</u> ssi il existe $x \in E$ tel que $E = E_x$.

L'exercice suivant donne quelques précisions sur $E_x$.

#### *Exercice 11*

**1°/** Montrer que $E_x = \mathrm{Vect}(u^i(x) / i \in \mathbb{N})$ (sous-espace vectoriel engendré par les $u^i(x)$).

**2°/** Si $x$ est non nul soit $p = \mathrm{Max}\{i \in \mathbb{N}$ / le système $(x, u(x), \ldots, u^{i-1}(x)$ est libre$\}$. Montrer que dim $E_x = p$.

Soit $u^p(x) = a_0x + a_1u(x) + \ldots + a_{p-1}u^{p-1}(x)$ ($a_k \in \mathbf{K}$). Montrer que le polynôme $P = X^p - a_{p-1}X^{p-1} - \ldots - a_0$ est le polynôme minimal et le polynôme caractéristique de la restriction $u/E_x$ de $u$ à $E_x$.

Quelle est la matrice de $u/E_x$ dans la base $(x, u(x), \ldots, u^{p-1}(x))$ ?

#### *Exercice 12 : théorème de Cayley-Hamilton*

**1°/** Soit $u \in L(E)$ et $F$ un sous-espace vectoriel de $E$ stable par $u$. Montrer que le polynôme caractéristique de $u/F$ divise celui de $u$.

**2°/** Démontrer le <u>*théorème de Cayley-Hamilton*</u> : $\chi(u) = 0$.

(Soit $x \in E - \{0\}$ et $\Pi$ le polynôme minimal et caractéristique (d'après Ex. 11, 2/) de la restriction de $u$ à $E_x$; donc $\Pi(u)(x) = 0$; de plus $\Pi$ divise $\chi$ d'après 1°/ donc $\chi(u)(x) = (Q\times\Pi)(u)(x) = Q(u)\circ\Pi(u)(x) = 0$).

#### *Exercice 13*

Soient $P_x$ et $P_y$ les polynômes minimaux de $u/E_x$ et $u/E_y$ pour $x$ et $y$ appartenant à $E$.

**1°/** Montrer que si les polynômes $P_x$ et $P_y$ sont premiers entre eux on a : $E_x \cap E_y = \{0\}$. Prouver que $P_x.P_y = P_z$ où $z = x + y$.

**2°/** Montrer qu'il existe un élément $x$ de $E$ tel que $\mu_u = P_x$.

**3°/** Montrer que si $E$ est réunion d'un nombre fini de sous-espaces vectoriels $F_i$ alors $E$ est égal à l'un des $F_i$. Retrouver le résultat de la question précédente.

**4°/** Déduire du 2°/ que $E_u$ est cyclique ssi $\chi_u = \mu_u$.

### 1.6.2 Théorème de Jordan

Une matrice $J_q = \begin{pmatrix} 0 & & \cdots & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$ (d'ordre $q$) est appelée <u>*matrice nipotente de Jordan*</u>. La matrice $J_q(\lambda) = \lambda \mathrm{I}_q + J_q$ est appelée <u>*matrice de Jordan*</u> d'ordre $q$.

**<u>Lemme</u> 1 :** soit $u$ un endomorphisme nilpotent d'indice $\nu$ de $E$. Il existe deux sous-espaces vectoriels $F$ et $G$ stables par $u$ tels que $E = F \oplus G$ et dim $F = \nu$.

**Lemme 2** (*Structure des endomorphismes nilpotents*) : soit $u$ un endomorphisme nilpotent d'ordre $\nu$ de $E$. Il existe des sous-espaces vectoriels $E_1, E_2, \ldots, E_r$ stables par $u$ et des bases $B_1, B_2, \ldots, B_r$ de $E_1, E_2, \ldots, E_r$ tels que $E = E_1 \oplus E_2 \oplus \ldots \oplus E_r$ et, dans la base $B_i$, la matrice de $u/E_i$ est une matrice de Jordan nilpotente $J_{p_i}$ avec $p_i = \dim E_i$ $(1 \leq i \leq r)$.

Démonstration du lemme 1 : soit ${}^t u$ la transposée de $u$ : c'est un endomorphisme de $E^*$ (dual de $E$) définie par $\langle {}^t u(f^*); x\rangle = \langle f^*; u(x)\rangle$ pour toute forme linéaire $f^*$ et tout $x$ de $E$. Comme on a $({}^t u)^p = {}^t(u^p)$ pour tout entier naturel $p$ ainsi que $u \neq 0$ ssi ${}^t u \neq 0$, ${}^t u$ est nilpotente d'indice $\nu$. On a donc ${}^t u^{\nu-1} \neq 0$ et par suite il existe $x \in E$ et $f^* \in E^*$ tels que $\langle {}^t u^{\nu-1}(f^*); x\rangle \neq 0$ soit $\langle f^*; u^{\nu-1}(x)\rangle \neq 0$.

On a donc $u^{\nu-1}(x) \neq 0$ et par conséquent le système $(x, u(x), \ldots, u^{\nu-1}(x))$ est libre (exercice 6). De même le système $(f^*, {}^t u(f^*), \ldots, {}^t u^{\nu-1}(f^*))$ est libre. Posons $F = \langle x, u(x), \ldots, u^{\nu-1}(x)\rangle$ et $G = \langle f^*, {}^t u(f^*), \ldots, {}^t u^{\nu-1}(f^*)\rangle^{\perp}$.

$F$ est un sous-espace vectoriel de $E$ de dimension $\nu$ stable par $u$. De même $\langle f^*, {}^t u(f^*), \ldots, {}^t u^{\nu-1}(f^*)\rangle$ est un sous-espace vectoriel de $E^*$ stable par ${}^t u$ de dimension $\nu$ donc son orthogonal $G$ est stable par $u$ et de dimension $n - \nu$ (en effet on voit facilement qu'un sous-espace vectoriel est stable par $u$ ssi son orthogonal est stable par ${}^t u$).

Montrons que $F \cap G = \{0\}$ ce qui prouvera que $E = F \oplus G$ et achèvera la démonstration de lemme 1.

Soit donc $y \in F \cap G$. Il existe des scalaires $a_0, a_1, \ldots, a_{\nu-1}$ tels que $y = \sum_{k=0}^{\nu-1} a_k u^k(x)$ et d'autre part $\langle {}^t u^j(f^*); y\rangle = 0$ ou $\langle f^*; u^j(y)\rangle = 0$ pour tout entier $j$ de $\{0, \ldots, \nu - 1\}$. Pour $j = \nu - 1$ il vient : $\langle f^*, a_0 u^{\nu-1}(x)\rangle = 0$ (car $u^p = 0$ pour $p \geq \nu$) soit $a_0 \langle f^*; u^{\nu-1}(x)\rangle = 0$ donc $a_0 = 0$ ($\langle f^*; u^{\nu-1}(x)\rangle$ étant non nul). En prenant ensuite $j = \nu - 2$ on montre de même que $a_1 = 0$ et de proche en proche tous les $a_j$ sont nuls, donc $y = 0$.

Démonstration du lemme 2 : avec les notations du lemme 1, la matrice de $u$ dans le base $B_1 = (x, u(x), \ldots, u^{\nu-1}(x))$ de $F$ est la matrice de Jordan nilpotente d'ordre $\nu$ et la restriction de $u$ au sous-espace vectoriel $G$ est nilpotente : on termine alors facilement par récurrence sur la dimension $n$ de $E$.

On déduit de ces deux lemmes le

**Théorème** (*décomposition de Jordan d'un endomorphisme*) : avec les hypothèses du théorème 1.4, il existe une base de $E$ où la matrice de $u$ est une matrice diagonale de matrices $J_h(\lambda_k)$ $(1 \leq k \leq p)$.

Fin de la Démonstration du théorème : reprenons les notations du théorème de 1.4 et soit $E = N_1 \oplus \ldots \oplus N_p$ la décomposition de $E$ en sous-espaces spectraux. Raisonnons dans $N_k$ : on applique le lemme 2 à la restriction $v_k$ de $u - \lambda_k \mathrm{Id}$ à $N_k$ qui est nilpotent et on obtient une base de $N_k$ dans laquelle la matrice de $v_k$ est une matrice diagonale de matrices nilpotentes de Jordan. Dans cette base la matrice de $u/N_k$ est une matrice diagonale de matrices de Jordan $J_h(\lambda_k)$. En « recollant » ces bases de $N_k$ on obtient une base de $E$ qui a la propriété voulue.

Les deux exercices suivants donnent des applications de ce théorème :

***Exercice 14***

Montrer qu'une matrice réelle $M$ est semblable à sa transposée (raisonner d'abord dans $M_n(\mathbb{C})$).

***Exercice 15***

Soit $A \in GL_n(\mathbb{C})$; montrer qu'il existe $B \in M_n(\mathbb{C})$ telle que $A = \exp(B)$.

### 1.6.3 Décomposition de $E$ somme directe de sous-espaces cycliques

**Théorème :** Soit $u \in L(E)$.

**(i)** Il existe une suite $F_1, \ldots, F_r$ de sous-espaces cycliques (donc stables par $u$) tels que $E = F_1 \oplus \ldots \oplus F_r$ ; si $P_i$ est le polynôme minimal de la restriction de $u$ à $F_i$ alors $P_i$ est multiple de $P_{i+1}$ $(1 \leq i \leq r-1)$; le polynôme minimal de $u$ est $P_1$ et son polynôme caractéristique $P_1 \times \ldots \times P_r$.

**(ii)** La suite de polynômes précédente est entièrement déterminée par $u$; deux endomorphismes sont semblables ssi la suite de polynômes associés sont égales.

La suite $(P_1, \ldots, P_r)$ uniquement déterminée par $u$ s'appelle *invariants de similitude* de $u$ (ou *facteurs invariants* de $u$).

Démonstration du théorème :

*Existence d'une décomposition* : d'après l'exercice 12 il existe $x \in E$ tel que $\mu = P_x$. Soit $E_x$ le sous-espace cyclique engendré par $x$. Supposons qu'on ait montré que $E_x$ a un supplémentaire $F$ stable par $u$ : $E = E_x \oplus F$. Le polynôme $\mu$ annule la restriction $u/F$ de $u$ à $F$ donc le polynôme minimal de $u/F$ divise $\mu$. On pose $\mu = P_1$ et on termine facilement par récurrence sur $n$.

Tout revient donc à montrer que $E_x$ possède un supplémentaire stable par $u$.

Posons $\mu = P_1^{\alpha_1}.P_2^{\alpha_2}....P_q^{\alpha_q}$ où les polynômes $P_k$ sont irréductibles et $\frac{\mu}{P_k} = P_1^{\alpha_1}....P_k^{\alpha_k - 1}....P_q^{\alpha_q}$.

Lemme 1 : il existe $(x, f^*) \in E \times E^*$ tel que $P_x = \mu = P_{f^*}$ et pour tout $j$ de $\{1, ... , q\}$ : $\langle f^*; p_j.x\rangle \neq 0$.

*Démonstration du lemme 1* : montrons que le système $(p_1.x, ... , p_q.x)$ est libre (on rappelle que si $P \in$ Erreur! Signet non défini.$[X]$, $P.x = P(u)(x)$). Supposons que $\sum_{k=1}^{q} a_k p_k.x = 0$. Pour $1 \leq j \leq q$, si on multiplie les deux membres par le polynôme $q_j = \frac{P_1...P_q}{P_j}$ il vient $a_k q_j p_j.x = 0$ (car si $k \neq j$ le polynôme $q_j p_k$ est un multiple de $\mu$). Comme $q_j p_j$ n'est pas un multiple de $\mu$ (car le facteur $P_j$ est la puissance $\alpha_j$ - 1) on a $q_j p_j.x \neq 0$ soit $a_j = 0$ et le système $(p_1.x, ... , p_q.x)$ est libre.

Il existe donc $f^* \in E^*$ telle que $\langle f^*; p_j.x\rangle = 1$ pour $1 \leq j \leq q$. Montrons que $P_{f^*} = \mu$.

On munit $E^*$ de sa structure de $\mathbf{K}[X]$-module grâce à ${}^t u$ (donc pour tout $P \in \mathbf{K}[X]$ et tout $f^*$ de $E^*$ : $P.f^* = P({}^t u)(f^*)$). Comme pour tout $z$ de $E$ $\langle \mu.f^*; z\rangle = \langle f^*; \mu.z\rangle = 0$, on a $\mu.f^* = 0$ donc $P_{f^*}$ divise $\mu$. Mais $\langle p_j.f^*; x\rangle = \langle f^*; p_j.x\rangle \neq 0$ donc on a $P_{f^*} = \mu$ d'où le lemme 1.

Posons $F = \langle {}^t u^k(f^*) / k \in \mathbb{N}\rangle^{\perp}$ et montrons que $E = E_x \oplus F$.

On a dim $E_x$ = d°$\mu = q$ et de même la dimension de $\langle {}^t u^k(f^*) / k \in \mathbb{N}\rangle$ est égale au degré de $P_{f^*}$ qui est aussi $q$ d'après le lemme précédent donc dim $F = n - q$.

D'autre part $\langle {}^t u^k(f^*) / k \in \mathbb{N}\rangle$ est stable par ${}^t u$ donc $F$ est stable par $u$. Pour avoir $E = E_x \oplus F$ il reste donc à montrer que $E_x \cap F = \{0\}$.

Soit donc $y \in E_x \cap F$. Il existe $Q \in \mathbf{K}[X]$ tel que $y = Q.x$ et pour tout $R$ de $\mathbf{K}[X]$ on a $\langle R.f^*; y\rangle = 0$ soit $\langle R.f^*; Q.x\rangle = 0$ ou $\langle f^*; RQ.x\rangle = 0$.

Lemme 2 : $x$ et $f^*$ étant choisis comme dans le lemme 1, supposons que pour tout $R \in \mathbf{K}[X]$ on ait $\langle f^*; RQ.x\rangle = 0$. Alors $\mu$ divise $Q$.

Admettons provisoirement le lemme. On a donc $\mu$ divise $Q$ donc $Q(x) = 0$ soit $y = 0$ ce qui achève la démonstration de l'existence de la décomposition.

D'après l'exercice 4 le polynôme caractéristique de $u$ est $P_1 \times \ ... \ \times P_r$.

*Démonstration du lemme 2* :

Soit $D$ le pgcd de $Q$ et de $\mu$. $\mathbf{K}[X]$ étant principal il existe $U$ et $V$ dans $\mathbf{K}[X]$ tels que $D = UQ + V\mu$. Supposons que d°$D <$ d°$\mu$. $D$ s'écrit $P_1^{\beta_1}.P_2^{\beta_2}...P_q^{\beta_q}$ avec $\beta_k \leq \alpha_k$ pour $1 \leq k \leq q$ et il existe $j \in \{1, ... , q\}$ tel que $\beta_j < \alpha_j$. Donc $D$ divise $p_j$ (on rappelle que $p_j = \frac{\mu}{P_j}$) i.e $p_j$ appartient à l'idéal $(D) = (Q) + (\mu)$ et il existe $U'$ et $V'$ dans $\mathbf{K}[X]$ tels que $p_j = U'Q + V'\mu$.

On écrit : $\langle f^*; p_j.x\rangle = \langle f^*; U'Q.x\rangle + \langle f^*; V'\mu.x\rangle = 0$ puisque $\langle f^*; U'Q.x\rangle = 0$ par hypothèse et $\langle f^*; V'\mu.x\rangle = 0$ ($\mu.x = 0$) ce qui est absurde car $\langle f^*; p_j.x\rangle \neq 0$.

*Unicité de la décomposition* : supposons que l'on ait une autre décomposition avec les conditions de l'énoncé : $E = G_1 \oplus ... \oplus G_p = F_1 \oplus ... \oplus F_r$ et soit $Q_i$ le polynôme minimal de $u/G_i$.

Comme $F_1$ et $G_1$ sont cycliques leur dimension est égale au degré de leur polynôme minimal (exercice 10, 2°/). Mais $\mu = \text{ppmc}(P_i) = P_1 = \text{ppmc}(Q_i) = Q_1$ (exercice 4, 1°/) donc dim $G_1$ = dim $F_1$. Si $p = 1$ alors $r = 1$. Si $p$ et $r$ sont > 1, le

polynôme minimal des restrictions de $u$ à $G_2 \oplus ... \oplus G_p$ et $F_2 \oplus ... \oplus F_r$ sont respectivement $Q_2$ et $P_2$ donc on a de même dim $G_2$ = dim $F_2$. On voit par récurrence que dim $G_k$ = dim $F_k$ pour $k \leq \text{Min}(p, r)$ et par conséquent $p = r$. Si $p = r = 1$ on a $F_1 = G_1 = E$ et l'unicité est démontrée. Soit donc $p = r \geq 2$.

Supposons que $(P_1, ..., P_r) \neq (Q_1, ..., Q_r)$ et soit $j$ le plus petit entier $k$ tels que $P_k \neq Q_k$. On a donc $j \geq 2$.

$P_j$ étant un multiple de $P_k$ pour $k \geq j$ on a :

$$P_j(u)E = P_j(u)F_1 \oplus ... \oplus P_j(u)F_{j-1} = P_j(u)G_1 \oplus ... \oplus P_j(u)G_{j-1} \oplus P_j(u)G_j \oplus ... \oplus P_j(u)G_r \quad (*).$$

Comme $P_i = Q_i$ pour $1 \leq i \leq j$-1 on a dim $F_i$ = dim $G_i$ ($F_i$ et $G_i$ étant deux espaces cycliques ayant même polynôme minimal). L'égalité (*) donne alors $P_j(u)G_j = ... = P_j(u)G_r = \{0\}$ et par conséquent $P_j$ est un multiples de $Q_j$.

On montrerait de même que $Q_j$ est un multiple de $P_j$ par conséquent $Q_j = P_j$ ce qui contredit la définition de $j$.

Cela démontre entièrement le (i).

**(ii)** $u$ étant donné les sous-espaces vectoriels $F_k$ sont déterminés de façon unique et $P_k$ est le polynôme minimal de $u/F_k$ qui sont donc déterminés de façon unique.

Si $P = a_0 + a_1X + ... + a_pX^p \in \mathbf{K}[X]$ notons $M(P)$ la matrice $\begin{pmatrix} 0 & & & a_0 \\ 1 & \ddots & & a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & a_{p-1} \end{pmatrix}$. D'après l'exercice 10 il existe une base de $E$ dans laquelle la matrice de $u$ est $\begin{pmatrix} M(P_1) & & \\ & \ddots & \\ & & M(P_r) \end{pmatrix}$ d'où il résulte que deux endomorphismes sont semblables ssi ils ont même invariants de similitudes.