Compléments d'algèbre linéaire

Cédric Lecouvey

Mastère II Tours-Orléans 2014-2015

Table des matières

1 Introduction

L'objectif de cours est l'étude de notions et résutats classiques concernant la réduction des endomorphismes d'espaces vectoriels en lien avec le calcul dans les algèbres de matrices. Ces notions ont été mises en place sous leur forme moderne au XIX et XX-ièmes siècles sous l'impulsion de mathématiciens tels que Sylvester, Hamilton, Cayley (XIX-ième) puis Jordan, Frobenius, Schur, Noether (XX-ième). Le Chapitre 2 est consacré à des rappels sur les notions très classiques d'algèbres de matrices et de polynômes annulateurs. Il expose aussi les principaux résultats du programme de Licence concernant la réduction des endomorphismes. Cependant le lecteur est supposé familier avec les notions d'espace vectoriel et de matrice qui ne sont pas réexposées ici. Dans le Chapitre 3, on introduit la notion d'endomorphisme cyclique et de matrice compagnon d'un polynôme. Le Chapitre 4 est consacré à la réduction de Frobenius des endomorphismes ainsi qu'à la notion d'invariants de similitude. Faute de temps, le lien avec la notion de module sur un anneau principal ne sera pas présenté dans ce cours. Nous renvoyons pour cela le lecteur par exemple à [2] et [3] pour des exposés complets sur le calcul des invariants d'un tel module. Dans le chapitre 5, on trouvera diverses applications de la réduction de Frobenius, la plus célèbre étant la réduction de Jordan des endomorphismes sur $\mathbb{C}$. Le chapitre 6 est une ouverture à la théorie des représentations des algèbres de dimension finie, tout particulièrement à celle des algèbre de matrices. On montre aussi qu'une algèbre simple de dimension finie sur $\mathbb{C}$ est isomorphe à une algèbre de matrices. Enfin, le Chapitre 7 présente le problème de Burnside sur les groupes de type fini et périodiques. On y démontre notamment le théorème de Schur selon lequel un tel groupe de matrices est nécessairement fini. Les méthodes de preuves mélangent des outils d'algèbre linéaire avec des éléments de théorie de Galois qui ont été étudiés en M1.

2 Quelques notations et rappels

2.1 Algèbres d'endomorphismes

Soit $\mathbb{K}$ un corps. Dans toute la suite E est un $\mathbb{K}$-espace vectoriel de dimension finie n. On note $\mathcal{L}(E)$ l'algèbre des endomorphismes de E dans E. C'est une $\mathbb{K}$-algèbre associative unitaire d'unité l'application identité id et de dimension n^2. Pour tout choix d'une base de E, l'algèbre $\mathcal{L}(E)$ s'identifie avec l'algèbre $\mathcal{M}_n(\mathbb{K})$ des matrices carrées de rang n à coefficients dans $\mathbb{K}$.

Plus généralement, dans la suite $\mathcal{A}$ désignera une $\mathbb{K}$-algèbre $\mathcal{A}$ de dimension finie unitaire. L'élément neutre pour la multiplication sera noté $\mathbf{1}$. Un idéal à gauche (resp. à droite) de $\mathcal{A}$ est un sous-espace vectoriel I tel que $aI \in I$ (resp. $Ia \in I$) pour tout $a \in \mathcal{A}$. Un idéal bilatère est un idéal simultanément à gauche et à droite. L'algèbre $\mathcal{A}$ de dimension finie est dite simple lorsque ses seuls iédeaux bilatères sont $\mathcal{A}$ et $\{0\}$.

Proposition 2.1 *L'algèbre $\mathcal{L}(E)$ est simple.*

Preuve : Si on fixe une base de E, il suffit de démontrer que les seuls idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbb{K})$. Si I est un idéal bilatère de $\mathcal{M}_n(\mathbb{K})$ non réduit à $\{0\}$, I contient une matrice M de rang $r \geq 1$. Il existe donc deux matrices inversibles P et Q telles que

$$PMQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = J_r.$$

Donc J_r est dans I mais alors la matrice élementaire $E_{11} = J_r E_{11}$ est aussi dans I. Notons $T_{1,i}$ la matrice transposant les coordonées 1 et i. Alors, $T_{1,i}E_{11}T_{1,i} = E_{i,i}$. Donc I contient toutes les matrices $E_{i,i}$ pour $i = 1, \ldots, n$. Finalement, $I_n = E_{1,1} + \cdots + E_{n,n}$ est dans I ce qui entraîne que $I = \mathcal{M}_n(\mathbb{K})$. □

2.2 Polynômes annulateurs

Soit $u \in \mathcal{L}(E)$. Pour tout polynôme $P \in \mathbb{K}[X]$ tel que $P(X) = a_n X^n + \cdots + a_1 X + a_0$, on note $P(u) = a_n u^n + \cdots + a_1 u + id$. L'application

$$\varphi_u : \begin{cases} \mathbb{K}[X] \to \mathcal{L}(E) \\ P \mapsto P(u) \end{cases}$$

est un morphisme d'algèbres. Comme $\mathbb{K}[X]$ est un anneau principal, son noyau $\ker \varphi_u$ est un idéal principal. Il existe donc un unique polynôme unitaire μ_u tel que $\ker \varphi_u = (\mu_u)$. On appelle μ_u le polynôme minimal de u. Comme $\mathbb{K}[X]$ est de dimension infinie et que $\mathcal{L}(E)$ est de dimension finie, φ_u ne peut pas être injective. Donc $\deg \mu_u \geq 1$. Notons $\mathcal{L}_u = \operatorname{Im} \varphi_u$.

Lemme 2.2 *L'algèbre $\mathcal{L}_u$ est de dimension $\deg \mu_u$ et $B = \{id, u, \ldots, u^{\deg(\mu_u)-1}\}$ est une base de $\mathcal{L}_u$.*

Preuve : Découle immédiatement de l'isomorphisme de $\mathbb{K}$-espaces $\mathbb{K}[X]/(\mu_u) \simeq \mathcal{P}_u$. □

Remarque 2.3 *Noter que si $P(u) = 0$ et e est un vecteur propre de u associé à la valeur propre λ, on a $P(u)(e) = P(\lambda)e = 0$. Donc λ est une racine de P. Ainsi tout polynôme annulateur de u admet les valeurs propres de u comme racines. En particulier, les valeurs propres de u sont des racines de μ_u. La réciproque est vraie et sera une conséquence du théorème de Cayley-Hamilton (voir ci-dessous).*

Lemme 2.4 (dit lemme des noyaux) *Soient P et Q deux polynômes de $\mathbb{K}[X]$ premiers entre eux. Alors*

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

Preuve : Comme A et B sont premiers entre eux dans l'anneau $\mathbb{K}[X]$ euclidien (et donc principal), il existe, d'après le théorème de Bezout, deux polynômes A et B tels que

$$PA + QB = 1$$

dans $\mathbb{K}[X]$. Nous avons donc $P(u)A(u) + Q(u)B(u) = id$ dans $\mathcal{L}(E)$. Soit $x \in \ker P(u) \cap \ker Q(u)$. L'égalité précédente entraîne que

$$x = A(u)P(u)(x) + B(u)Q(u)(x) = 0.$$

Donc $\ker P(u) \cap \ker Q(u) = \{0\}$. Soit $x \in \ker PQ(u)$. Alors $Q(u)A(u)P(u)(x) = Q(u)P(u)A(u)(x) = 0$ donc $A(u)P(u)(x) \in \ker Q(u)$. De même $B(u)Q(u)(x) \in \ker P(u)$. Comme $x = A(u)P(u)(x) + B(u)Q(u)(x)$, cela montre que $\ker PQ(u) = \ker P(u) + \ker Q(u)$ de plus la somme est directe puisque $\ker P(u) \cap \ker Q(u) = \{0\}$. □

Théorème 2.5 *Soit $u \in \mathcal{L}(E)$. Alors u est diagonalisable si et seulement si μ_u est scindé à racines simples.*

Preuve : Si u est diagonalisable dans une base B de vecteurs propres pour les valeurs propres distinctes $\{\lambda_1, \ldots, \lambda_r\}$, soit M la matrice de u dans B. La matrice M est annulée par $P(X) = (X - \lambda_1) \cdots (X - \lambda_r)$ et donc μ_u / P. Puisque chaque $\lambda_i, i = 1, \ldots, r$ est une racine de μ_u, on a en fait $\mu_u = P$ qui est bien scindé à racines simples.
Supposons $\mu_u(X) = (X - \lambda_1) \cdots (X - \lambda_r)$ scindé à racines simples. D'après le lemme des noyaux, nous avons

$$E = \ker \lambda_u(u) = \bigoplus_{i=1}^{r} \ker(u - \lambda_r id) = \bigoplus_{i=1}^{r} E_{\lambda_i}$$

où les E_{λ_i} sont les espaces propres de u. Donc u est bien diagonalisable. □

Le polynôme caractéristique de u noté χ_u est quant à lui défini par

$$\chi_u(X) = \det(u - Xid)$$

il s'agit donc d'un polynôme de degré n de coefficient dominant $(-1)^n$. On trouve dans certains livre une définition un peu différente de χ_u : $\chi_u(X) = \det(Xid - u)$.

Théorème 2.6 *Soit $u \in \mathcal{L}(u)$. Les deux assertions suivantes sont équivalentes :*

1. *Il existe une base B de E dans laquelle la matrice de u est triangulaire supérieure*

$$M_B = \begin{pmatrix} \lambda_1 & * & \cdot & \cdot & * \\ 0 & \lambda_2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & * \\ 0 & \cdot & \cdot & 0 & \lambda_n \end{pmatrix}.$$

2. *Le polynôme χ_u est scindé dans $\mathbb{K}$.*

Preuve : L'implication (1) ⇒ (2) est immédiate par calcul direct $\det \chi_u(X) = \det(M - XI_n)$ où I_n est la matrice identité. Pour montrer que (2) ⇒ (1), on raisonne par récurrence sur la dimendion n. Comme les valeurs propres de u sont exactement les racines de χ_u qui est scindé, u admet au moins une valeur propre λ_1 associée à un vecteur propre e_1. Soit F un sous-espace de E tel que $E = \mathbb{K}e_1 \oplus F$. Pour toute base B_F de F, $B_F \cup \{e_1\}$ est une base de E dans laquelle la matrice de u prend la forme

$$M_1 = \begin{pmatrix} \lambda_1 & a \\ 0 & M_2 \end{pmatrix}$$

où $a \in \mathbb{K}$ et M_2 est une matrice carrée d'ordre $n - 1$. De plus, $\chi_u(X) = \det(M - XI_n) = (X - \lambda_1)\chi_{M_2}(X)$. Soit $u_2 \in \mathcal{L}(F)$ l'endomorphisme dont la matrice dans la base B_F est M_2. Puisque $\chi_{M_2}(X)$ est scindé, d'après l'hypothèse de récurrence, il existe une base $B' = \{e_2, \ldots, e_n\}$ de F dans laquelle la matrice de u_2 est triangulaire supérieure. Alors la matrice de u dans la base $B = \{e_1, \ldots, e_n\}$ de E est également triangulaire supérieure ce qui démontre le théorème par récurrence. □

Théorème 2.7 (Cayley Hamilton) *χ_u est un polynôme annulateur de u, autrement dit μ_u divise χ_u.*

Preuve : Supposons tout d'abord que $\chi_u = (X-\lambda_1)\cdots(X-\lambda_n)$ est scindé dans $\mathbb{K}$. D'après le théorème précédent, il existe une base $B = \{e_1, \ldots, e_n\}$ de E dans laquelle la matrice M_B est triangulaire supérieure. Pour tout $k = 1, \ldots, n$, notons $N_k = (M_B - \lambda_1 I_n)\cdots(M_B - \lambda_k I_n)$. Montrons par récurrence que $N_k(e_1) = \cdots = N_k(e_k) = 0$ pour tout $k = 1, \ldots, n$. Comme e_1 est un vecteur propre pour λ_1, on a bien $N_1(e_1) = 0$. Suppsosons $N_{k-1}(e_1) = \cdots = N_{k-1}(e_{k-1}) = 0$ pour $k > 1$. Comme $N_k = N_{k-1}(M_B - \lambda_k I_n) = (M_B - \lambda_k I_n)N_{k-1}$, on obtient $N_k(e_1) = \cdots = N_k(e_{k-1}) = 0$. Puisque M_B est triangulaire supérieure, $(M_B - \lambda_k I_n)(e_k) \in vect\langle e_1, \ldots, e_{k-1}\rangle$. Ainsi $N_k(e_k) = 0$ ce qui démontre notre propriété par récurrence. Finalement pour $n = k$, cela donne $N_n = \chi_u(M_B) = 0$ donc $\chi_u(u) = 0$.
Supposons maintenant que χ_u n'est pas scindé dans $\mathbb{K}$. Soit $\mathbb{L}$ un coprs de décomposition de χ_u au dessus de $\mathbb{K}$. Dans $\mathbb{L}$, le polynôme χ_u est scindé. Soit M la matrice de u dans une base de E. D'après ce qui précède, la matrice M, vue comme une matrice à coefficients dans $\mathbb{L}$, vérifie $\chi_u(M) = 0$. Comme $\chi_u(M)$ est une matrice à coefficients dans $\mathbb{K}$, l'égalité est en fait vraie dans $\mathcal{M}_n(\mathbb{K})$ (et on a bien $\chi_u(u) = 0$. $\square$

Remarque 2.8 *Comme χ_u est de degré n, nous avons* $\deg(\mu_u) \leq n$. *Par définition, les racines de χ_u sont les valeurs propres de u. Comme μ_u/χ_u et que toutes les valeurs propres sont racines de μ_u (car μ_u est un polynôme annulateur de u), il s'ensuit que les valeurs propres de u sont exactement les racines de μ_u.*

Soit x un vecteur de E. L'application φ_x

$$\varphi_x : \begin{cases} \mathbb{K}[X] \to E \\ P \mapsto P(u)(x) \end{cases}$$

est linéaire. On note $E_x = \{P(u)(x) \mid P \in \mathbb{K}[X]\}$ son image. Bien que φ_x ne soit évidemment pas un morphisme d'anneau, $\ker \varphi_x$ est un idéal de $\mathbb{K}[X]$. En effet si $P \in \ker \varphi_x$ et $Q \in \mathbb{K}[X]$, nous avons $QP(u)(x) = Q(u) \circ P(u)(x) = 0$. Il s'agit donc là aussi d'un idéal principal de $\mathbb{K}[X]$ et il existe donc un unique polynôme unitaire μ_x tel que $\ker \varphi_x = (\mu_x)$. Puisque que $\mu_u(u)(x) = 0$, on a $\mu_u \in (\mu_x)$ et donc

$$\mu_x \text{ divise } \mu_u \text{ pour tout } x \in E.$$

Remarque 2.9 *Si x n'est pas nul,* $\deg(\mu_x) \geq 1$. *On retrouve donc que* $\deg \mu_u \geq 1$.

Lemme 2.10 *Pour tout $x \in E$, l'espace E_x est stable sous l'action de u et $B_x = (x, u(x), \ldots, u^{\deg(\mu_x)-1}(x)\}$ forme une base de E_x.*

Preuve : Découle immédiatement de l'isomorphisme $\mathbb{K}[X]/(\mu_x) \simeq E_x$. $\square$

2.3 Exercices

Exercice 2.11 *Soit f un endomorphisme de E où E est un $\mathbb{K}$ e.v. de dimension finie. On suppose que $rg(f) = 1$. Donner une condition nécessaire et suffisante pour que f soit diagonalisable.*

Exercice 2.12 *Soit $\mathcal{A}$ une sous-algèbre sur le corps $\mathbb{K}$ de dimension finie. Comment définir la notion de polynôme minimal d'un élément de $\mathcal{A}$?*

Exercice 2.13 *Soit I un intervalle de $\mathbb{R}$ et $\mathcal{A}$ une sous-algèbre de dimension finie de $\mathcal{C}^0(I,\mathbb{R})$. Montrer que $A = \mathbb{R}\mathbf{1}$ où $\mathbf{1}$ est la fonction identiquement égale à 1.*

Exercice 2.14 *On considère un $\mathbb{C}$-espace vectoriel de dimension finie$E$. Soit $u \in L(E)$ et $\ell \in \mathbb{N}^*$.*

1. *On suppose u inversible, montrer que u est diagonalisable ssi u^ℓ est diagonalisable.*
2. *Dans le cas général, montrer que u est diagonalisable ssi $\ker u = \ker u^\ell$.*

Exercice 2.15 *Le but de l'exercice est de redémontrer le théorème de Cayley Hamilton. Soit $u \in \mathcal{L}(E)$ où E est de dimension finie. Il s'agit de montrer que pour tout $x \in E$, $\chi_u(u)(x) = 0$.*

1. *Soit F un s.e.v de E stable par u. Montrer que $\chi_{u_{|F}}$ divise χ_u.*
2. *Soit $x \in E \setminus \{0\}$. Justifier que*

$$p = \max\{r \in \mathbb{N}^* \mid \{x, u(x), \dots, u^{r-1}(x)\} \text{ est libre}\}$$

   est bien définie et qu'il existe $a_0, \dots, a_{p-1}$ dans $\mathbb{K}$ tels que $u^p(x) = a_0 x + a_1 u(x) \cdots + a_{p-1}u^{p-1}(x)$.
3. *Justifier que $F = \text{vect}\{x, u(x), \dots, u^{p-1}(x)\}$ est stable par u. On note $v = u_{|F}$.*
4. *Montrer que $\chi_v(u)(x) = 0$ et conclure.*

Exercice 2.16 *Soint U et V diagonalisables dans $M_n(\mathbb{C})$. Le but de l'exercice est de montrer que l'endomorphisme $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ tel que $\Phi(M) = UM - MV$ est diagonalisable.*

1. *Montrer que les endomorphismes $\delta : M \longmapsto UM$ et $\gamma : M \longmapsto MV$ sont diagonalisables.*
2. *Vérifier que γ et δ commuttent et conclure.*

Exercice 2.17 *Montrer que l'ensemble des matrices diagonalisables dans $M_n(\mathbb{C})$ est dense dans $M_n(\mathbb{C})$ (on pourra utiliser la trigonalisation et construire, pour chaque matrice triangulaire supérieure T, une suite de matrices diagonalisables T_n qui converge vers T. Le résultat subsiste-t-il dans $M_n(\mathbb{R})$ (utiliser la continuité de l'application qui à $M \in M_2(\mathbb{R})$ associe $\Delta(M)$ le discriminant de son polynôme caractéristique ?*

Exercice 2.18 *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Montrer que A est nilpotente si et seulement si $tr(A^k) = 0$ pour tout $k = 1, \dots, n$.*

3 Endomorphismes cycliques

3.1 Un résultat fondamental

Définition 3.1 *Un endomorphisme $u \in \mathcal{L}(E)$ est dit* cyclique *lorsqu'il existe un vecteur $x \in E$ tel que $E_x = E$.*

Nous avons vu que pour tout $x \in E$, on a μ_x / μ_u. L'objectif de ce paragraphe est de démontrer qu'il existe au moins un vecteur x dans E tel que $\mu_x = \mu_u$.

Lemme 3.2 *Supposons qu'il existe un polynôme irréductible P tel que $\mu_u = P^\alpha A$ avec $\alpha > 0$, A et P premiers entre-eux. Alors, il existe $x \in E$ tel que $\mu_x = P^\alpha$.*

Preuve : Comme P et A sont premiers entre eux, on peut utiliser le lemme des noyaux ce qui donne la décomposition en somme directe

$$E = \ker P^\alpha(u) \oplus \ker A(u).$$

Maintenant soit x non nul dans $\ker P^\alpha(u)$. Comme $P^\alpha(u)(x) = 0$, le polynôme μ_x divise P^α. Supposons que pour tout x non nul dans $\ker P^\alpha(u)$, μ_x divise en fait $P^{\alpha-1}$. Cela implique que $P^{\alpha-1}(u)$ s'annule sur $\ker P^\alpha(u)$. Considérons l'endomorphisme $v = P^{\alpha-1}A(u)$. Il s'annule sur $\ker A(u)$ mais aussi sur $\ker P^\alpha(u)$ d'après notre hypothèse. Donc $v = P^{\alpha-1}A(u)$ est nul ce qui contredit le fait $\mu_u = P^\alpha A$ est le polynôme minimal de u. On a donc l'existence d'un vecteur x non nul tel que $\mu_x = P^\alpha$. □

Lemme 3.3 *Soient x et y deux vecteurs de E tels que μ_x et μ_y soient premiers entre eux. Alors $\mu_{x+y} = \mu_x\mu_y$.*

Preuve : Observons tout d'abord que

$$\mu_x\mu_y(u)(x+y) = \mu_x(u)\mu_y(u)(x+y) = \mu_y(u)\mu_x(u)(x) + \mu_x(u)\mu_y(u)(y) = 0$$

puisque $\mu_x(u)(x) = \mu_y(u)(y) = 0$. Donc μ_{x+y} divise $\mu_x\mu_y$. Par ailleurs $\mu_{x+y}(u)(x+y) = 0$ donc $\mu_{x+y}(u)(x) = -\mu_{x+y}(u)(y)$. On en déduit que

$$\mu_y(u)\mu_{x+y}(u)(x) = -\mu_y(u)\mu_{x+y}(u)(y) = -\mu_{x+y}(u)\mu_y(u)(y) = 0.$$

Ainsi μ_x divise $\mu_y\mu_{x+y}$. Mais comme μ_y et μ_x sont premiers entre-eux, cela signifie que μ_x divise μ_{x+y}. Par symétrie, on a aussi que μ_y divise μ_{x+y}. Finalement, puisque μ_x et μ_y sont premiers entre-eux, on obtient que $\mu_x\mu_y$ divise μ_{x+y} ce qui termine la preuve du lemme. □

Théorème 3.4 *Soit u un endomorphisme de $\mathcal{L}(E)$. Il existe un vecteur x de E tel que $\mu_x = \mu$.*

Preuve : Décomposons $\mu = P_1^{\alpha_1} \times \cdots \times P_r^{\alpha_r}$ en produit de facteurs premiers deux à deux distincts. D'après le Lemme 3.2, il existe des vecteurs $x_1, \ldots, x_r$ tels que $\mu_{x_i} = P_i^{\alpha_i}$ pour tout $i = 1, \ldots, r$. Le Lemme 3.3 et une récurrence immédiate montrent que $\mu_{x_1+\cdots+x_r} = \mu_u$. □

3.2 Condition de cyclicité

Proposition 3.5 (cyclicité et polynôme minimal) *Pour tout $u \in \mathcal{L}(E)$, on a les équivalences*

$$u \text{ est cyclique} \iff \deg \mu_u = n \iff \chi_u = (-1)^n \mu_u$$

Preuve : Posons $d = \deg(\mu_u)$. Supposons que u soit cyclique. Il existe x dans E tel que $B = \{x, u(x), \ldots, u^{n-1}(x)\}$ soit une base de E. Posons $\mu_u = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Alors

$$u^d(x) + a_{d-1}u^{d-1}(x) + \cdots + a_0 x = 0$$

Si $d < n$, cela donne une combinaison linéaire de vecteurs de B nulle à coefficients non tous nuls, donc une contradiction avec le fait que B est une base. On a bien $d = n$.
Supposons maintenant que $d = n$, nous avons alors μ_u/χ_u, χ_u est de degré n et enfin μ_u et $(-1)^n\chi_u$ sont des polynômes unitaires. Donc $\chi_u = (-1)^n\mu_u$.
Pour terminer, supposons $\chi_u = (-1)^n\mu_u$. D'après le Théorème 3.4, il existe un vecteur x dans E tel que $\mu_x = \mu_u$. Supposons qu'il existe des scalaires $b_0, \ldots, b_{n-1}$ tels que

$$\sum_{k=0}^{n-1} b_k u^k(x) = 0.$$

Alors $B(u)(x) = 0$ où B est le polynôme $B(X) = b_nX^n + \cdots + b_1 + b_0$. Donc $\mu_x = \mu_r$ divise B. Or $\deg(B) < n$ et $\deg(\mu_r) = n$. Cela entraîne que $B = 0$ ce qui signifie que $B = \{x, u(x), \ldots, u^{n-1}(x)\}$ est une base de E. □

3.3 Matrice compagnon et cyclicité

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polynôme de $\mathbb{K}[X]$ de degré n. On note

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

la matrice compagnon de P (les coefficients non représentés sont nuls). On vérifie facilement que le polynôme caractéristique de $\mathcal{C}(P)$ est égal à $(-1)^nP$.

On dit qu'une matrice A est cyclique si l'endomorphisme correspondant à A dans la base canonique est cyclique.

Proposition 3.6 (cyclicité et matrice compagnon) *Soit $u \in \mathcal{L}(E)$.*

1. *Si u est cyclique, alors u est semblable à la matrice compagnon de son polynôme minimal.*
2. *Si u est semblable à la matrice compagnon du polynôme unitaire P, alors u est cyclique de polynôme minimal P.*

Preuve : Supposons que u est cyclique et soit x tel que $B = \{x, u(x), \ldots, u^{n-1}(x)\}$ forme une base de E. D'après la Proposition 3.5, μ_r est de degré n. On peut poser

$$\mu_r(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

On a bien sûr $u(u^k(x)) = u^{k+1}(x)$ pour tout $k = 0, \ldots, n-2$. Par ailleurs, $\mu_r(u)(x) = 0$ implique que $u(u^{n-1})(x) = -a_{n-1}u^{n-1}(x) - \cdots - a_0x$. Dans la base B, la matrice de u est donc bien la matrice compagnon de μ_r.
Réciproquement supposons que u est semblable à la matrice compagnon du polynôme unitaire P. Il existe alors une base $B = \{e_0, \ldots, e_{n-1}\}$ de E dans laquelle la matrice de u vaut $\mathcal{C}(P)$. On a donc $u(e_k) = e_{k+1}$ pour tout $k = 0, \ldots, n-2$ Cela donne $e_k = u^k(e_0)$ pour tout $k = 0, \ldots, n-1$ et u est cyclique. Comme le polynôme caractéristique de $\mathcal{C}(P)$ est égal à $(-1)^nP$ et puisque u est cyclique semblable à $\mathcal{C}(P)$, la Proposition 3.5 entraîne que $P = \mu_r$.□

Remarque 3.7 *D'après la proposition précédente, le polynôme minimal de $\mathcal{C}(P)$ est égal à P.*

3.4 Exercices

Exercice 3.8 *Montrer qu'un endomorphisme est simultanément diagonalisable et cyclique si et seulement si il admet n valeurs propres dictinctes.*

Exercice 3.9 *Notons $\mathcal{C}_n$ des endomorphismes cycliques de $\mathcal{M}_n(\mathbb{C})$.*

1. *En considérant les applications $\theta_x : M \to \det(x, Mx, \ldots, M^{n-1}x)$ de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$ où $x \in \mathbb{C}^n$, démontrer que $\mathcal{C}_n$ est un ouvert de $\mathcal{M}_n(\mathbb{C})$.*
2. *Justifier le fait que toute matrice de $\mathcal{M}_n(\mathbb{C})$ est limite d'une suite de matrices dont les valeurs propres sont distinctes et en déduire que $\mathcal{C}_n$ est dense dans $\mathcal{M}_n(\mathbb{C})$.*

Exercice 3.10 *En utilisant l'exercice précédent, montrer que l'application $\mu : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}[X]$ qui à A associe μ_A n'est pas continue (on justifiera le fait que $\chi : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}[X]$ qui à A associe χ_A est continue et on considérera $\mu - \chi$).*

Exercice 3.11 *On dit que $P \in \mathbb{C}[X]$ est un polynôme de Sylvester lorsque chacun de ses coefficients est de module ≤ 1. On note Z_n l'ensemble de toutes les racines possibles des polynômes de Syvester de degré au plus n.*

1. *En utilisant les formules de Newton pour le lien entre coefficients et racines, montrer que Z_n est fini.*
2. *Soit $\xi \in Z_n$. Montrer que pour tout entier $k \geq 0$, $\xi^k \in Z_n$ (penser à la notion de matrice compagnon).*
3. *En déduire que les éléments de Z_n sont des racines de l'unité (théorème dû à Kronecker).*

4 Invariants de similitude et réduction de Frobenius

D'après le paragraphe précédent, tous les endomorphismes ne sont pas cycliques. Cependant, nous allons montrer que pour tout endomorphisme u de $\mathcal{P}(E)$, il existe une décomposition de E en sous-espaces stables par u où la restriction de u est cyclique. Ces espaces ne sont pas uniques mais ils définissent une suite de polynômes qui elle est unique : ce sont les invariants de similitude de u.

4.1 Suite des invariants de similitude

Théorème 4.1 *Soit $u \in \mathcal{L}(E)$. Il existe une suite $F_1, \ldots, F_r$ de sous-espaces de E stables par u non réduits à $\{0\}$ telle que*

1. *$E = F_1 \oplus \cdots \oplus F_r$,*
2. *chaque F_i est stable par u et $u_{|F_i}$ est cyclique,*
3. *en posant $\mu_i = \mu_{|F_i}$, on a la suite de divisibilités $\mu_r / \mu_{r-1} / \cdots / \mu_1$ et $\mu_1 = \mu_u$.*
   Par ailleurs, la suite $\mu_1, \ldots, \mu_r$ ne dépend que de u et pas des sous-espaces F_i. On l'appelle la suite des invariants de similitude de u.

Preuve :

1 Existence : on procède par récurrence sur n. Si $n = 1$, on a $r = 1$ et l'existence souhaitée est évidente. Supposons que cette existence soit vraie en dimension $< n$. D'après le Théorème 3.4, il existe un vecteur x non nul tel que $\mu_u = \mu_x$. Notons $d = \deg(\mu_u)$. Alors E_x est un sous-espace de E

de dimension $d > 0$ stable sous l'action de u. On pose $F_1 = E_x$. Nous avons, que la restriction de u à F_1 est cyclique et donc d'après la Proposition 3.6, $\mu_{|F_1} = \mu_1 = \mu_u$. L'idée est alors de trouver un supplémentaire de F_1 stable par u. Pour cela posons $e_k = u^k(x)$ pour tout $k = 0, \dots, d-1$. Alors $\{e_0, \dots, e_{d-1}\}$ est une base de F_1. Complétons là en une base $B = \{e_0, \dots, e_n\}$ de E. Considérons alors e_d^* le d-ième vecteur de la base duale de B. Il s'agit de l'application linéaire qui associe à tout vecteur de E sa d-ième coordonnée dans la base B. Posons

$$\Gamma = \text{vect}\langle e_d^* \circ u^k \mid k \in \mathbb{N}\} \text{ et } G = \Gamma^\circ = \{y \in E \mid e_d^* \circ u^k(y) = 0 \ \forall k \in \mathbb{N}\}$$

son dual dans E. Si $y \in G$, $e_d^* \circ u^k(u(y)) = e_d^* \circ u^{k+1}(y) = 0$ pour tout $k \in \mathbb{N}$ donc G est stable par u. Montrons que $E = F_1 \oplus G$. Soit $y \in F_1 \cap G$. Comme $\{e_0, \dots, e_{d-1}\}$ est une base de F_1, il existe un entier m tel que

$$y = \lambda_0 e_0 + \cdots + \lambda_m e_m \text{ et } \lambda_m \neq 0.$$

Alors $u^{d-m}(y) = \lambda_0 e_d + \cdots + \lambda_m e_d$ et $e_d^* \circ u^{d-m}(y) = \lambda_m \neq 0$ ce qui contredit le fait que $y \in G$. Donc $F_1 \cap G = \{0\}$. Pour montrer que $\dim G + \dim F_1 = n$, considérons l'application linéaire

$$\theta : \left\{ \begin{array}{c} \mathcal{L}_u \to \Gamma \\ P(u) \mapsto e_d^* \circ P(u) \end{array} \right.$$

Il est clair que θ est surjective. Si P est non nul dans $\ker\theta$, on peut écrire $P(u) = a_0 id + \cdots + a_p u^p$ avec $a_p \neq 0$. Posons $y = u^{d-p}(e_0)$. Alors $P(u)(y) = a_0 e_{d-p} + \cdots + a_p e_d$. Mais alors $e_d^* \circ P(u)(y) = a_p \neq \{0\}$ et donc $e_d^* \circ P(u) \neq \{0\}$ ce qui donne une contradiction. Ainsi $\ker\theta = \{0\}$ et θ est un isomorphisme. On a donc $\dim\Gamma = \dim\mathcal{L}_u = d$ d'après le Lemme 2.2. Cela donne bien $\dim G = n - \dim\Gamma = n - d$ et donc $E = F_1 \oplus G$. Notons finalement que $\mu_{u|G}$ divise $\mu_u = \mu_{u|F_1}$. On peut donc appliquer notre hypothèse de récurrence et obtenir l'existence de la décomposition ainsi que celle de la famille de polynômes annoncée.

2 Unicité : Supposons l'existence de deux suites de sous-espaces $F_1, \dots, F_r$ et $G_1, \dots, G_s$ avec $r \geq s$ vérifiant les conditions du théorème. Notons $P_i = \mu_{u|F_i}$ et $Q_j = \mu_{u|G_j}$. On a déjà $Q_1 = P_1 = \mu_r$ et comme les restrictions de u à F_1 et G_1 sont cycliques, $\dim F_1 = \dim G_1 = d$. Supposons les deux suites disctinctes. Il existe alors un indice $j \geq 2$ minimal tel que $P_j \neq Q_j$. En effet dans le cas contraire $P_i = Q_i$ pour tout $i = 1, \dots, s$ ce qui est impossible car $\sum_{i=1}^r \deg(P_i) = \sum_{j=1}^s \deg(Q_j) = \dim E$ et $r > s$ car les deux suites sont distinctes. Comme $P_j(F_{j+k}) = 0$ pour $k = 0, \dots, r$, on a

$$\begin{array}{c} P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1}) \text{ et} \\ P_j(u)(E) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_{j-1}) \oplus P_j(u)(G_j) \oplus \cdots \oplus P_j(u)(G_s). \end{array} \quad (1)$$

Or $P_a = Q_a$ pour tout $a = 1, \dots, j-1$ donc $u_{|F_a}$ et $u_{|G_a}$ sont semblables puisqu'il s'agit d'endomorphismes cycliques (voir Proposition 3.6). On en déduit que $\dim P_j(u)(F_a) = \dim P_j(u)(G_a)$ pour $a = 1, \dots, j-1$. En utilisant (1), on voit donc que $0 = \dim P_j(u)(G_j) = \cdots = \dim P_j(u)(G_s)$ ce qui implique notamment que Q_j divise P_j. Par symétrie, on obtient de même que P_j divise Q_j et donc $P_j = Q_j$ contrairement à notre hypothèse. Cela montre bien que les deux suites de sous-espaces sont égales. □

4.2 Réduction de Frobenius

Théorème 4.2 *Si $\mu_1, \dots, \mu_r$ sont les invariants de similitudes de u, il existe une base B de E dans laquelle*

$$M_B(u) = \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}.$$

De plus

$$\mu_r = \mu_1 \text{ et } \chi_u = \mu_1 \cdots \mu_r.$$

Preuve : L'existence de la base B s'obtient directement à partir du Théorème 4.1 et en utilisant que la matrice d'un endomorphisme cyclique est semblable à la matrice compagnon de son polynôme minimal. Pour le calcul de χ_u, on observe que $\chi_u = \chi_{\mathcal{C}(\mu_1)} \cdots \chi_{\mathcal{C}(\mu_r)} = \mu_1 \cdots \mu_r$ puisque le polynôme caractéristique de $\mathcal{C}(P)$ vaut P. □

Remarque 4.3 *Soit $u \in \mathcal{L}(E)$. Si $P_1, \dots, P_r$ est une suite de polynômes unitaires tels que $P_r / \cdots / P_1$ et si il existe une base B de E dans laquelle*

$$M_B(u) = \begin{pmatrix} \mathcal{C}(P_1) & & \\ & \ddots & \\ & & \mathcal{C}(P_r) \end{pmatrix}$$

alors u est cyclique d'invariants de similitude $P_1, \dots, P_r$. En effet la décomposition par blocs détermine une partition $B = B_1 \cup \cdots \cup B_r$ de la base B. Si on note $F_i = \text{vect}(B_i)$, on retrouve les conditions du Théorème 4.1 et on conclut par unicité des invariants de similitude.

Nous allons maintenant caractériser les endomorphismes semblables. Pour cela, nous aurons besoin d'un lemme intermédiaire. Soit $u \in \mathcal{L}(E)$ et $v \in GL(E)$. Notons $g = vuv^{-1}$. On se donne un sous-espace F stable par u.

Lemme 4.4 *Nous avons les proprietés suivantes :*

1. *$v(F)$ est stable par g,*
2. *$u_{|F}$ est cyclique si et seulement si $g_{|v(F)}$ est cyclique,*
3. *$\mu_{u_{|F}} = \mu_{g_{|v(F)}}$.*

Preuve : Soit $x \in F$, alors $g(v(x)) = vu(x) \in v(F)$ puisque $u(x) \in F$ ce qui montre le point 1. Pour le point 2, on note $p = \deg(\mu_{u_{|F}})$ et on observe que $\{x, \dots, u^{d-1}(x)\}$ est une base de F si et seulement si $\{v(x), \dots, vu^{d-1}(x)\}$ est une base de $v(F)$. C'est suffisant puisque $vu^k(x) = (vuv^{-1})^k(v(x)) = g^k(v(x))$ pour tout $k = 0, \dots, d-1$. Puisque $P(g) = vP(u)v^{-1}$ pour tout polynôme $P \in \mathbb{K}[X]$, $P(g) = 0$ si et seulement si $P(u) = 0$. Comme $P(g_{|v(F)}) = P(g)_{|v(F)}$ et $P(u_{|F}) = P(u)_{|F}$, on a bien $\mu_{u_{|F}} = \mu_{g_{|v(F)}}$ comme annoncé dans le point 3. □

Théorème 4.5 *Deux endomorphismes de $\mathcal{L}(E)$ sont semblables si et seulement si ils ont les mêmes invariants de similitudes.*

Preuve : Le Théorème 4.2 entraîne que deux endomorphismes ayant les mêmes invariants de similitude sont semblables. Réciproquement considérons $u \in \mathcal{L}(E)$, $v \in GL(E)$ et $g = vuv^{-1}$. Soit $F_1, \ldots, F_r$ une famille de sous-espaces comme dans le Théorème 3.4. Puisque v est inversible on a

$$E = F_1 \oplus \cdots \oplus F_r = v(F_1) \oplus \cdots \oplus v(F_r).$$

En utilisant le lemme précédent, les $v(F_i)$ sont stables par g, chaque restriction $g_{|v(F_i)}$ est cyclique , $\mu_{u_{|F_i}} = \mu_{g_{|v(F_i)}}$ et donc

$$\mu_{g_{|v(F_r)}} / \cdots / \mu_{g_{|v(F_1)}} = \mu_g = \mu_u.$$

Par unicité de la décomposition, les polynômes $\mu_{u|F_i}$ sont aussi les invariants de similitude de g. □

Remarque 4.6 *Il existe des algorithmes permettant le calcul effectif des invariants de similitude d'une matrice. La plupart d'entre-eux utilisent la notion de module sur un anneau principal : les invariants de similitude de A sont les facteurs invariants de la matrice $A - XI_n$. Nous renvoyons par exemple à [2] pour une exposition détaillée de ces notions.*

4.3 Exercices

Exercice 4.7 *Soient E et F des espaces vectoriels de dimension p et q sur $\mathbb{C}$, $f : E \to F$ et $g : F \to E$ deux applications linéaires.*

1. *Soit $\lambda \neq 0$. Montrer que λ est valeur propre de $f \circ g$ ssi λ est valeur propre de $g \circ f$.*
2. *Pour une valeur propre λ non nulle de $f \circ g$ et de $g \circ f$, montrer que les sous-espaces caractéristiques associés sont isomorphes.*
3. *Que peut-on en déduire pour $\chi_{f \circ g}$ et $\chi_{g \circ f}$?*

Exercice 4.8 *Soit A une matrice 3×3 dont les invariants de similitudes sont $P_1 = (X - 2)$ et $P_2 = (X - 2)(X - 4) = X^2 - 6X + 8$. Montrer que A est semblable à*

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -8 \\ 0 & 1 & 6 \end{pmatrix}.$$

Exercice 4.9 *Montrer qu'en dimension ≤ 3 deux endomorphismes sont semblables ssi ils ont même polynômes minimal et caractéristique. Est-ce vrai en dimension $n \geq 4$?*

Exercice 4.10 *En utilisant la décomposition de Frobenius, montrer qu'un endomorphisme u de rang r posséde un polynôme annulateur de degré au plus $r + 1$.*

5 Applications

5.1 Commutant d'un endomorphisme cyclique

Pour tout $u \in \mathcal{L}(E)$, on note $\mathrm{Comm}(u)$ le commutant de u défini par

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

Il est clair que $\mathrm{Comm}(u)$ est une sous-algèbre de $\mathcal{L}(E)$ contenant au moins tous les polynômes $P(u)$ avec $P \in \mathbb{K}[X]$.

Proposition 5.1 *L'endomorphisme u est cyclique si et seulement si* $\mathrm{Comm}(u) = \mathbb{K}[u]$ *i.e. le commutant de u se réduit aux polynômes en u.*

Preuve : Supposons que u soit cyclique. Il existe un vecteur x dans E tel que $E = E_x$. Soit $f \in \mathrm{Comm}(u)$. Le vecteur $f(x) \in E$ s'écrit sous la forme $f(x) = P(u)(x)$ où $P \in \mathbb{K}[X]$. Montrons que $f = P(u)$. Soit $y \in E$, on peut écrire $y = Q(u)(x)$ avec $Q \in \mathbb{K}[X]$

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

où la deuxième égalité utilise le fait que f commute avec tout polynôme en u. On a donc bien $f = P(u)$ un polynôme en u.
Réciproquement, suppàsons $\mathrm{Comm}(u) = \mathbb{K}[u]$. On applique le Théorème 3.4 pour obtenir une décomposition

$$E = F_1 \oplus \cdots \oplus F_r$$

avec les bonnes propriéteés. Nous allons montrer que $r = 1$ ce qui implique que u est cyclique. Supposons $r > 1$. Soit π la projection sur $F_2 \oplus \cdots \oplus F_r$ de noyau F_1. Comme F_1 et $F_2 \oplus \cdots \oplus F_r$ sont stables par u, nous avons $\pi \circ u = u \circ \pi$ c'est à dire que $\pi \in \mathrm{Comm}(u)$. Il existe donc un polynôme P tel que $\pi = P(u)$. Comme $\pi_{|F_1} = 0$, nous avons $P(u_{|F_1}) = P(u)_{|F_1} = 0$. Cela implique que μ_u divise P. Mais comme les invariants de similitude $\mu_1, \ldots, \mu_r$ sont tous des diviseurs de μ_r, on a $P(u_{|F_i}) = 0$ pour tout $i = 1, \ldots, r$ car $u_{|F_i}$ a pour polynôme minimal μ_i. Mais alors

$$\pi = P(u) = P(u_{|F_1}) + \cdots + P(u_{|F_r}) = 0.$$

Donc $F_2 \oplus \cdots \oplus F_r = \{0\}$ ce qui est impossible car les espaces F_i dans la décomposition du Théorème 3.4 ne sont pas réduits à $\{0\}$. □

5.2 Réduction de Jordan

Un bloc de Jordan associée $\lambda \in \mathbb{K}$ est une matrice carrée de la forme

$$J = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}.$$

Théorème 5.2 *Supposons que $\mathbb{K}$ est algébriquement clos. Soit $u \in \mathcal{L}(E)$. Alors il existe une base de E dans laquelle la matrice de u prend la forme*

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

où chaque matrice $J_a, a = 1, \ldots, r$ est un bloc de Jordan associé à une valeur propre de u, deux blocs pouvant être associés à la même valeur propre.

Preuve : Puisque $\mathbb{K}$ est algébriquement clos, μ_u est scindé dans $\mathbb{K}$ et on peut le factoriser sous la forme

$$\mu_u(X) = (X-\lambda_1)^{\alpha_1} \cdots (X-\lambda_m)^{\alpha_m}$$

où les $\lambda_1, \ldots, \lambda_m$ sont les valeurs propres disctinctes de u. D'après le lemme des noyaux, on a alors

$$E = \ker(u-\lambda_1 id)^{\alpha_1} \oplus \cdots \oplus \ker(u-\lambda_m id)^{\alpha_1}$$

où les espaces $C_{\lambda_k} = \ker(u-\lambda_k id)^{\alpha_k}$ sont les sous-espaces caractéristiques de u. Comme $(u-\lambda_1 id)^{\alpha_k}$ est un polynôme en u, C_{λ_k} est stable par u et il suffit de démontrer le théorème sur chaque C_λ avec λ valeur propre de u. Soit donc λ une telle valeur propre et α sa multiplicité dans μ_u. Par définition de C_λ, $u_\lambda := (u-\lambda id)_{|C_\lambda}$ est nilpotent sur C_λ et $u_\lambda^\alpha = 0$. On peut alors appliquer le Théorème 4.2 à u_λ vu comme un endomorphisme de C_λ. Il existe donc une base B_λ de C_λ telle que la matrice de u_λ dans B_λ soit de la forme

$$M_\lambda = \begin{pmatrix} \mathcal{C}(\mu_1) & & \\ & \ddots & \\ & & \mathcal{C}(\mu_r) \end{pmatrix}$$

où $\mu_1, \ldots, \mu_r$ sont les invariants de similitude de u_λ. Puisque u_λ est nilpotent, ses invariants de similitude sont des puissances de X et donc, chaque matrice compagnon dans M_λ est de la forme

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

En permuttant l'ordre des vecteurs de B_λ, on obtient une base B'_λ de C_λ dans laquelle la matrice de $u_\lambda = u_{|C_\lambda} - \lambda id_{C_\lambda}$ est de la forme

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

et dans cette même base B'_λ, la matrice de $u_{|C_\lambda}$ prend la forme

$$\begin{pmatrix} \begin{pmatrix} \lambda & 1 & & \\ \vdots & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \begin{pmatrix} \lambda & 1 & & \\ \vdots & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} \end{pmatrix}.$$

Finalement la base évoquée dans le théorème est la réunion disjointe des bases $B'_{\lambda_1}, \ldots, B'_{\lambda_m}$. □

5.3 Matrices semblables et extensions de corps

Supposons que $\mathbb{L}$ est un extension du corps $\mathbb{K}$. Alors $\mathcal{M}_n(\mathbb{K})$ peut être considére comme une sous-algèbre de $\mathcal{M}_n(\mathbb{L})$.

Proposition 5.3 *Soit $M \in \mathcal{M}_n(\mathbb{K})$. Alors la suite des invariants de similitude de M est la même dans $\mathbb{K}[X]$ et dans $\mathbb{L}[X]$.*

Preuve : Notons $\mu_1, \ldots, \mu_r$ les invariants de similitude de M dans $\mathbb{K}[X]$. D'après le Théorème 4.2, il existe une matrice inversible P à coefficients dans $\mathbb{K}$ telle que

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

où $\mu_r / \cdots / \mu_1$. Cette relation reste vraie dans $\mathcal{M}_n(\mathbb{L})$ ce qui permet de conclure d'après la Remarque 4.3. □

La proposition précédente combinée avec le Théorème 4.5 implique le

Corollaire 5.4 *Deux matrices sont semblables dans $\mathcal{M}_n(\mathbb{K})$ si et seulement si elles le sont dans $\mathcal{M}_n(\mathbb{L})$.*

5.4 Exercices

Exercice 5.5 *Justifier que le Théorème 5.2 reste vrai pour tout endomorphisme u tel que χ_u soit scindé.*

Exercice 5.6 (Décomposition de Dunford) *Soit $u \in \mathcal{L}(E)$ tel que χ_u soi scindé, montrer qu'il existe une unique paire $(d, n) \in \mathcal{L}(E)^2$ avec d diagonalisable et n nilpotente telle que $u = d + n$ et $nd = dn$ (pour l'unicité, on pourra utiliser la décomposition en sous-espaces caractéristiques).*

Exercice 5.7 *Déterminer la réduite de Jordan d'une matrice* 3×3 *dont les invariants de similitude sont* $P_1 = (X-2)$ *et* $P_2 = (X-2)(X-4)$.

Exemple 5.8 *Montrer que la réduite de Jordan d'une matrice* 4×4 *dont le seul invariant de similitude est* $P_1 = (X-2)^2(X-4)^2$ *est :*

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

Exemple 5.9 *Soit* $A \in \mathcal{M}_n(\mathbb{C})$. *Donner une condition nécessaire et suffisante pour que* M *et* $2M$ *soient semblables.*

Exercice 5.10 *Soit* $u \in \mathcal{L}(E)$ *dont la réduite de Jordan est constituée d'un seul bloc* $J_n(\lambda)$ *de taille* n. *On pose* $v = u - \lambda id$. *Soit* $x \in E \setminus \ker v^n$. *Montrer que* $B = (x, g(x), \ldots, g^{n-1}(x))$ *est une base de* E *dans laquelle la matrice de* u *est égale à* $J_n(\lambda)$.

Exercice 5.11 *On suppose que* $A \in \mathcal{M}_n(\mathbb{C})$ *avec* $\chi_A(X) = (-1)^n(X-\lambda)^n$, $\mu_A(X) = (X-\lambda)^\beta$ *et* $\dim V(\lambda) = \gamma$. *Montrer que*

$$\frac{n}{\beta} \leq \gamma \leq 1 + \alpha - \beta.$$

6 Représentations d'algèbres

Dans ce chapitre, $\mathcal{A}$ est une $\mathbb{K}$-algèbre de dimension finie associative et unitaire. On peut par exemple songer à l'algèbre $\mathcal{L}(E)$ des endomorphimes d'un espace vectoriel de E où à l'algèbre $\mathbb{K}[G]$ d'un groupe fini G. Une représentation (ρ, E) de dimension finie de $\mathcal{A}$ est la donnée d'un $\mathbb{K}$-espace vectoriel V et d'une action ρ linéaire de $\mathcal{A}$. Plus formellement, on se donne un morphisme unitaire (c'est-à-dire que $\rho(1) = Id$)

$$\rho : \mathcal{A} \to \mathcal{L}(E)$$

et pour tout $a \in \mathcal{A}$, l'endomorphisme $\rho(a)$ de E est l'action de a sur V. On note pour alleger les notations $a \cdot v = \rho(a)(v)$ pour tout $v \in V$. On a donc

$$a \cdot (\lambda v + \mu v') = \lambda a \cdot v + \mu a \cdot v'$$

pour tout $a \in \mathcal{A}$, $v, v' \in E$ et $\lambda, \mu \in \mathbb{K}$. Les résultats qui suivent montrent que la théorie des représentations des algèbres de matrices est très simple (comparativement à celles de groupes finis par exemple). Noter que les sous-représentations de $\mathcal{A}$ (c'est-à-dire celles pour lesquelles E est un sous-espace de $\mathcal{A}$) sont précisément les idéaux à gauche de $\mathcal{A}$, l'action est alors la multiplication dans $\mathcal{A}$. En effet si I est un tel idéal, c'est un $\mathbb{K}$-sous-espace de $\mathcal{A}$ stable par la multiplication à gauche

$$\begin{cases} \mathcal{A} \to \mathcal{L}(I) \\ a \longmapsto \begin{cases} I \to I \\ x \longmapsto ax \end{cases} \end{cases}$$

Un autre exemple de représentation est la représentation dite standard $\mathbb{K}^n$ de l'algèbre de matrices $\mathcal{M}_n(\mathbb{K})$.

Lemme 6.1 *En tant que représentation de $\mathcal{M}_n(\mathbb{K})$, $\mathbb{K}^n$ est irréducible.*

Preuve : si $V \subset \mathbb{K}^n$ est une sous-représentation non réduite à $\{0\}$, elle contient un vecteur $v \neq 0$. L'orbite de v sous l'action du groupe $GL_n(\mathbb{C})$ est $V \setminus \{0\}$ ce qui montre que $V = \mathbb{K}^n$. □

6.1 Représentations d'une algèbre de matrices

Théorème 6.2

1. *Soit $\rho : \mathcal{M}_n(\mathbb{K}) \to \mathcal{L}(E)$ une représentation de dimension finie de l'algèbre des matrices $\mathcal{M}_n(\mathbb{K})$. Alors, il existe une base de E dans laquelle, pour tout $a \in \mathcal{A}$, la matrice de $\rho(a)$ est diagonale par blocs de la forme*

$$M = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}.$$

   En particulier, n divise $\dim V$.

2. *A isomorphisme près, les représentations irréductibles de $\mathcal{M}_n(\mathbb{K})$ sont la représentation triviale $\{0\}$ et la représentation standard. Toute représentation E se décompose en somme directe de représentations irréducitbles sous la forme*

$$E = U_1 \oplus \cdots \oplus U_r$$

   avec $U_k \simeq \mathbb{K}^n$ pour tout $k = 1, \ldots, r$.

Preuve :
1 : On rappelle que l'algèbre $\mathcal{M}_n(\mathbb{K})$ est engendrée par les matrices élémentaires $E_{i,j}$. La multiplication des matrices élémentaires vérifie

$$E_{i,j}E_{k,l} = E_{i,l}\delta_{j,k}.$$

L'idée consiste à regarder les images $\rho(E_{i,j})$. Remarquons tout d'abord que

$$I_n = E_{1,1} + \cdots + E_{n,n}.$$

Notons $P_i = \rho(E_{i,i})$. Puisque $E_{i,i}^2 = E_{i,i}$ et $E_{i,i}E_{j,j} = 0$ pour $i \neq j$, $P_1, \ldots, P_n$ est une famille de projecteurs tels que $P_iP_j = 0$ pour $i \neq j$. Ainsi si on note $V_i = \operatorname{Im} P_i$, nous aurons

$$E = V_1 \oplus \cdots \oplus V_n.$$

Considérons $i \neq j$ et l'application linéaire $P_{i,j} = \rho(E_{i,j}) : V_j \to V_i$. Alors $id_{|V_j} = P_{j|V_j} = \rho(E_{j,i})\rho(E_{i,j})_{|V_j}$ ce qui montre que $P_{i,j}$ est injective et que $\operatorname{Im} P_{i,j} \subseteq V_i$ comme annoncé. On a aussi $id_{|V_i} = P_{i|V_i} = \rho(E_{i,j})\rho(E_{j,i})_{|V_i}$ ce qui implique la surjectivité de $P_{i,j}$. Finalement, nous obtenons que $P_{i,j}$ est un isomorphime d'espaces vectoriels.
Soit $(e_1^{(1)}, \ldots, e_r^{(1)})$ une base de V_1. Pour tout $i = 1, \ldots, n$, notons $(e_1^{(i)}, \ldots, e_r^{(i)})$ l'image de cette base par l'isomorphisme $P_{i,j}$, autrement dit $e_k^{(i)} = P_{i,1}e_k^{(1)}$ pour tout $k = 1, \ldots, r$ et tout $i = 1, \ldots, n$. Posons pour tout $k = 1, \ldots, n$

$$U_k = \operatorname{vect}\langle e_k^{(1)}, e_k^{(2)}, \ldots, e_k^{(n)}\rangle.$$

Nous avons

$$\rho(E_{k,l})(e_k^{(i)}) = \begin{cases} e_k^{(i)} \text{ si } i = k = l, \\ e_k^{(i+1)} \text{ si } i < n, k = i+1 \text{ et } l = i, \\ e_k^{(1)} \text{ si } i = n, k = 1 \text{ et } l = n \\ 0 \text{ sinon.} \end{cases}$$

ce qui montre que chaque espace U_k est stable par l'action de $\mathcal{M}_n(\mathbb{K})$. De plus $\rho(\mathcal{M}_n(\mathbb{K}))(e_k^{(1)})$ engendre la base $B_k = \{e_k^{(1)}, e_k^{(2)}, \ldots, e_k^{(n)}\}$. Nous disposons donc d'un morphisme d'algèbres

$$\rho_k : \begin{cases} \mathcal{M}_n(\mathbb{K}) \to \mathcal{L}(U_k) \\ M \mapsto \rho(M)_{|U_k} \end{cases}$$

non nul puisque $\rho(\mathcal{M}_n(\mathbb{K}))(e_k^{(1)})$ engendre la base B_k. Comme les seuls idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbb{K})$, $\ker \rho_k = \{0\}$. Par ailleurs, $\mathcal{L}(U_k) \simeq \mathcal{M}_n(\mathbb{K})$ puisque $\dim U_k = n$. Finalement ρ_k est un isomorphisme et donc U_k est une représentation irréductible de $\mathcal{M}_n(\mathbb{K})$ (elle est isomorphe à $\mathbb{K}^n$). On obtient donc la décomposition de E en composantes irréductibles

$$E = U_1 \oplus \cdots \oplus U_r.$$

Dans la base $B = B_1 \cup \cdots \cup B_r$, on obtient l'écriture matricielle souhaitée.
2 : Si E est irréducible, nous avons $r = 1$ et $E = U_1$ est isomorphe à la représentation standard de $\mathcal{M}_n(\mathbb{K})$.

6.2 Algèbres simples de dimension finie

Proposition 6.3 *Soit $\mathcal{A}$ une $\mathbb{C}$-algèbre de dimension finie et (ρ, E) une représentation irréductible de $\mathcal{A}$.*

1. *Fixons $x \in E$ non nul. Alors pour tout vecteur x' non nul dans E, il existe $a \in \mathcal{A}$ tel que $x' = a \cdot x$.*
2. *Fixons $l \in E^*$ non nul. Alors pour tout l' non nul dans E^*, il existe $a \in \mathcal{A}$ tel que $l' = l(a \cdot x)$.*
3. *Si $u \in \rho(\mathcal{A})$ est de rang ≥ 2, il existe $u' \in \rho'(\mathcal{A})$ tel que $0 < rg(u') < rg(u)$.*

Preuve :
1 : Pour tout $x \in E$ non nul, l'espace $\mathcal{A} \cdot x$ est stable par $\mathcal{A}$ et non réduit à $\{0\}$ puisqu'il contient $\mathbf{1} \cdot x = \mathbf{1}$. Il s'agit donc d'une sous-représentation de E et comme E est irréductible, nous avons $\mathcal{A} \cdot x = E$.
2 : Considérons $B = \{l \circ \rho(a) \mid a \in \mathcal{A}\} \subset E^*$ le dual de E. Pour tout $\alpha \in \mathcal{A}$, $B^\circ = \{x \in E \mid l \circ \rho(a)(x) = 0, \forall a \in \mathcal{A}\}$ est stable par $\rho(\alpha)$. Comme B contient $l = \rho(\mathbf{1}) \circ l$, $B \neq \{0\}$ et donc $B^\circ \neq E$. Il s'ensuite que $B^\circ = \{0\}$ et $B = E^*$ ce qui démontre le point 2.
3 : Posons $u = \rho(\alpha)$ avec $\alpha \in \mathcal{A}$. Comme u est de rang au moins 2, il existe x et y dans E tels que $(u(x), u(y))$ soit libre. Puisque $u(x) \neq 0$, il existe d'après le point 1 élément $a \in \mathcal{A}$ tel que $y = a \cdot u(x)$. La restriction $u \circ \rho(a)_{|\operatorname{Im} u}$ est non nulle car $u \circ \rho(a)(u(x)) = u \circ (a \cdot u(x)) = u(y) \neq 0$. Puisque le corps de base est $\mathbb{C}$, $u \circ \rho(a)_{|\operatorname{Im} u}$ possède donc au moins une valeur propre λ. Notons $v = (u \circ \rho(a) - \lambda \mathbf{1})_{|\operatorname{Im} u}$. On a alors $\operatorname{Im} v \subsetneq \operatorname{Im} u$ et donc $\operatorname{Im}(v \circ u) \subset \operatorname{Im} v \subsetneq \operatorname{Im} u$. De plus $v \circ u(x) = u \circ \rho(a) \circ u(x) - \lambda u(x) = u(y) - \lambda u(x) \neq 0$ puisque $u(y)$ et $u(x)$ sont libres. Cela montre que

$$v \circ u = u \circ \rho(a) \circ u - \lambda u = \rho(\alpha a \alpha - \lambda \alpha) \in \rho(\mathcal{A})$$

est non nul de rang strictement inférieur à celui de u ce qui termine la preuve. □

Théorème 6.4 (Burnside) *Supposons $\mathbb{K} = \mathbb{C}$. Soit (ρ, E) une représentation irréductible de $\mathcal{A}$. Alors $\rho(\mathcal{A}) = \mathcal{L}(E)$, autrement dit les actions des éléments de $\mathcal{A}$ coincident exactement avec tous les endomorphismes de E.*

Preuve : Si $\dim E = \{0\}$, le théorème est immédiat. Sinon, $\mathcal{L}(E)$ est engendré en tant qu'espace vectoriel par les applications linéaires de rang 1. Nous allons montrer que $\rho(\mathcal{A})$ contient toutes ces applications linéaires.
Pour montrer qu'il en contient bien une, on part de $u = \rho(\mathbf{1}) = id_E$. Si $\dim V = \{1\}$, u convient. Sinon, on applique le point 3 de la proposition précédente ce qui fournit par récurrence l'endomorphisme $\varphi = \rho(\alpha)$ avec $\alpha \in \mathcal{A}$ de rang 1 cherché.
Comme φ est de rang 1, il existe $v \in E$ et $l \in E^*$ tel que $\varphi = l(\cdot)v$. Soit $\varphi' = l'(\cdot)v'$ un autre endomorphisme de rang 1 de E. D'après les points 1 et 2 de la proposition précédente, il existe a et b dans $\mathcal{A}$ tels que $v' = a \cdot v$ et $l' = l \circ \rho(b)$. On a alors pour tout $x \in E$

$$\varphi'(x) = l'(x)v' = \underbrace{l \circ \rho(b)(x)}_{\in \mathbb{C}} \underbrace{\rho(a)(v)}_{\in E} = \rho(a)(l \circ \rho(b)(x)v)) =$$
$$\rho(a)(\varphi(\rho(b)(x))) = \rho(a)(\rho(\alpha)(\rho(b)(x))) = \rho(a\alpha b)(x)$$

et finalement $\varphi' = \rho(a\alpha b)$. Ainsi $\rho(\mathcal{A})$ contient bien touts les endomorphimes de rang 1 ce qui termine la preuve. □

On rappelle que $\mathcal{A}$ est simple lorsque ces seuls idéaux bilatères sont $\mathcal{A}$ et $\{0\}$.

Théorème 6.5 (Wedderburn) *Soit $\mathcal{A}$ une $\mathbb{C}$-algèbre simple de dimension finie. Alors, il existe un entier n tel que*

$$\mathcal{A} \simeq \mathcal{M}_n(\mathbb{C}).$$

Preuve : Nous avons vu que les sous-représentations de $\mathcal{A}$ correspondent aux idéaux à gauche de $\mathcal{A}$. Comme $\mathcal{A}$ est de dimension finie et est un idéal à gauche, on peut choisir un idéal à gauche I de $\mathcal{A}$ non réduit à $\{0\}$ de dimension minimale. On dispose alors d'une représentation par multiplication à gauche

$$\rho_I : \left\{ \begin{array}{c} \mathcal{A} \to I \\ a \mapsto \left\{ \begin{array}{c} I \to I \\ x \mapsto ax \end{array} \right. \end{array} \right.$$

irréductible puisque I est de dimension minimale. Le théorème de Burnside ci-dessus impose donc que $\rho_I(\mathcal{A}) = \mathcal{L}(I)$. Maintenant, comme $\ker \rho_I$ est un idéal bilatère de l'algèbre simple $\mathcal{A}$, nous avons $\ker \rho_I = \{0\}$ ou $\ker \rho_I = \mathcal{A}$. Or $\rho_I(\mathbf{1}) = id_I$ n'est pas nul donc $\ker \rho_I \neq \mathcal{A}$ et ρ_I est injective. Cela montre que $\mathcal{A} = \mathcal{L}(I) \simeq \mathcal{M}_n(\mathbb{C})$ où $n = \dim I$. □

6.3 Algèbres semi-simples sur $\mathbb{C}$

La $\mathbb{C}$-algèbre $\mathcal{A}$ de dimension finie est dite semi-simple lorsqu'il existe une décomposition

$$\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$$

de $\mathcal{A}$ en somme directe de sous-algèbres simples. Attention, cette notion de somme directe de sous-algèbres est plus forte que la notion de somme directe d'espaces vectoriels (qui ne tient pas compte

du produit). Il faut comprendre que chaque élément de $\mathcal{A}$ se décompose de façon unique sous la forme $a = a_1 + \cdots + a_r$ avec $a_i \in \mathcal{A}_i$ et si $a' = a'_1 + \cdots + a'_r$ est la décomposition de a' on a

$$aa' = a_1a'_1 + \cdots + a_ra'_r$$

avec $a_ia'_i \in \mathcal{A}_i$ pour tout $i = 1, \ldots, r$. En particulier, chaque $\mathcal{A}_i$ est un idéal bilatère de $\mathcal{A}$. Certains auteurs parlent d'ailleurs plutôt de produit direct d'algèbres que de somme directe.

Corollaire 6.6 (du théorème de Wedderburn) *Si $\mathcal{A}$ est une $\mathbb{C}$-algèbre semisimple, il existe des entiers $n_1, \ldots, n_r$ tels que*

$$\mathcal{A} \simeq \mathcal{M}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathcal{M}_{n_r}(\mathbb{C})$$

en tant que $\mathbb{C}$-algèbres.

6.4 Exercices

Exercice 6.7 *On considère G un groupe fini et $\mathbb{C}[G]$ l'algèbre du groupe G. Que peut-on dire du groupe G si l'algèbre $\mathbb{C}[G]$ est simple ?*

Exercice 6.8 *Soit $\mathcal{A}$ est une $\mathbb{C}$-algèbre semi-simple de dimension finie. Montrer que toute sous-algèbre de $\mathcal{A}$ et toute algèbre quotient de $\mathcal{A}$ est semi-simple.*

Exercice 6.9 *Soit $\mathcal{A}$ est une $\mathbb{C}$-algèbre semi-simple de dimension finie. En utilisant l'exercice précédent, montrer les équivalences entre*

1. *L'algèbre $\mathcal{A}$ est semisimple.*
2. *Toute représentation de dimension finie de $\mathcal{A}$ se décompose comme la somme directe de représentations irréductibles.*

Exercice 6.10 *En utilisant les résultats de ce cours et ceux de celui de théorie des représentations, montrer que l'algèbre $\mathbb{C}[G]$ d'un groupe fini est semi-simple. En déduire que*

$$\mathbb{C}[G] \simeq \mathcal{M}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathcal{M}_{n_r}(\mathbb{C})$$

où $n_1, \ldots, n_r$ sont les degrés des représentations irréductibles du groupe G sur $\mathbb{C}$.

7 Problème de Burnside pour les groupes de matrices

7.1 Le problème de Burnside

Définition 7.1 *soit G un groupe.*

1. *On dit que G est de type fini lorsqu'il est engendré par un nombre fini d'éléments.*
2. *On dit que G est périodique si pour tout g dans G, il existe un entier m tel que $g^m = 1$.*
3. *On dit que G est d'exposant fini si il existe un entier m tel que $g^m = 1$ pour tout g dans G.*

On prendra garde à l'ordre des quantificateurs dans les deux dernières définitions. Il est clair que d'après le théorème de Lagrange sur les groupes, tout groupe fini est d'exposant fini $m = |G|$. Bien sûr, il existe des groupes non périodiques (et donc infinis). Par exemple $G = \mathbb{Z}$. Le problème de Burnside est le suivant :

Problème 1 (dit de Burnside) : Un groupe *de type fini et périodique* est-il fini ?

On peut aussi se poser le problème plus contraint suivant :

Problème 2 : Un groupe *de type fini et d'exposant fini* est-il fini ?

Dans la suite, nous allons particulièrement étudier le cas où G est un sous-groupe du groupe des matrices inversibles $GL_n(\mathbb{C})$ de $\mathcal{M}_n(\mathbb{C})$. Nous présenterons des résultats dus à Burnside et Schur pour des sous-groupes de $GL_n(\mathbb{C})$. Le résultat de Burnside répond par l'affirmative au problème 2 pour de tels groupes. Il est légèrement antérieur à celui de Schur qui répond par l'affirmative au problème 1 pour les sous-groupes des groupes de matrices impliquant donc le résultat de Burnside.

Pour des groupes qui ne sont pas des sous-groupes de matrices (ou de façon équivalente qui n'admettent pas de réprésentation fidèle), il a été démontré par Grigorchuk en 1980 que la réponse au problème 1 est négative en général. La réponse au problème 2, n'est pas encore totalement élucidée. Actuellement, on connaît des groupes infinis de type fini et d'exposant ≥ 13 (Ivanov). Mais que se passe-t-il pour les groupes de type fini et d'exposant plus petit que 13 ?

7.2 Théorème de Burnside

Lemme 7.2 *Soit $u \in \mathcal{M}_n(\mathbb{C})$. Alors u est nilpotent si et seulement si $tr(u^p) = 0$ pour tout $1 \leq p \leq n$.*

Preuve : voir Exercice 2.18. □

Théorème 7.3 (Burnside) *Tout sous-groupe de $GL_n(\mathbb{C})$ de type fini et d'exposant fini est fini.*

Preuve : Soit G un tel groupe d'exposant e. Le $\mathbb{C}$-espace vectoriel $\mathcal{A} = vect\langle G\rangle$ de $\mathcal{M}_n(\mathbb{C})$ est une sous-algèbre unitaire de dimension finie et comme G est de type fini, il existe une famille finie $G_1, \ldots, G_m$ d'éléments du groupe G génératrice de l'algèbre $\mathcal{A}$. On considère l'application

$$\theta : \left\{ \begin{array}{c} G \to \mathbb{C}^m \\ M \mapsto (tr(MG_1, \ldots, MG_m)) \end{array} \right.$$

et nous allons montrer qu'elle est injective. Supposons donc A et B dans G tels que $\theta(A) = \theta(B)$. Comme la famille $G_1, \ldots, G_m$ engendre l'algèbre $\mathcal{A}$, nous avons $tr(AC) = tr(BC)$ pour tout $C \in \mathcal{A}$. Montrons par récurrence que pour tout entier $k \geq 0$, $tr((AB^{-1})^k) = n$. Pour $n = 0$, c'est clair. Supposons la propriété vraie pour $k - 1 > 0$. Alors

$$tr((AB^{-1})^k) = tr(AB^{-1}(AB^{-1})^{k-1}) = tr(BB^{-1}(AB^{-1})^{k-1}) = tr((AB^{-1})^{k-1}) = n$$

où on a utilisé l'égalité $tr(AC) = tr(BC)$ avec $C = B^{-1}(AB^{-1})^{k-1}$ et l'hypothèse de récurrence. Montrons maintenant que $AB^{-1} - I_n$ est nilpotent. Nous avons pour tout $1 \leq p \leq n$

$$tr((AB^{-1} - I_n)^p) = \sum_{k=0}^{p} \binom{p}{k} tr((AB^{-1})^k)(-1)^{p-k} = n \sum_{k=0}^{p} \binom{p}{k} (-1)^{p-k} = (1-1)^p = 0.$$

On peut donc en déduire que $AB^{-1} - I_n$ est nilpotent en appliquant le lemme précédent.
Montrons que $AB^{-1} - I_n$ est diagonalisable. Comme A et B sont dans G, AB^{-1} aussi. Donc $X^e - 1$ est un polynôme annulateur de AB^{-1} scindé dans $\mathbb{C}$ et à racines simples (ce sont les racines e-ième de l'unité). Donc AB^{-1} est diagonalisable et comme I_n est diagonale dans n'importe quelle base, $AB^{-1} - I_n$ est diagonalisable.
Pour terminer, il suffit d'observer qu'un endomorphisme diagonalisable et nilpotent est nul. Donc $A = B$ et θ est une injection de G dans S_e^m où S_e est l'ensemble de toutes les sommes possibles de n racines e-ième de l'unité. Cela découle du fait que chaque matrice MG_i est annulée par $X^e - 1$ et donc ses valeurs propres sont des racines e-ième de l'unité. Ainsi $tr(MG_i)$ est une somme de racines e-ièmes de l'unité. Comme S_e est fini, S_e^m aussi et on a contruit une injection de G dans un ensemble fini. Cela montre que G est lui aussi fini. □

7.3 Théorème de Schur

Nous aurons besoin de deux lemmes qui utilisent des élements essentiels de la théorie de Galois.

Lemme 7.4 *Soit $\mathbb{K}$ une extension de $\mathbb{Q}$ de degré d et $P \in \mathbb{K}[X_1, \ldots, X_n]$. Il existe un polynôme $\overline{P} \in \mathbb{Q}[X_1, \ldots, X_n]$ de degré $d\deg(P)$ tel que pour tout n-uplet $(z_1, \ldots, z_n) \in \mathbb{C}^n$*

$$P(z_1, \ldots, z_n) = 0 \Rightarrow \overline{P}(z_1, \ldots, z_n).$$

Preuve : L'extension $\mathbb{K}$ est de degré fini donc d'après le théorème de l' élément primitif, il existe un complexe θ_1 tel que $\mathbb{K} = \mathbb{Q}(\theta_1)$. De plus, si P_1 est le polynôme minimal de θ_1 alors $\deg(P_1) = d$. Soient $\theta_2, \ldots, \theta_d$ les autres racines de P_1 (elles sont toutes distinctes car P_1 est irréductible dans $\mathbb{Q}$ qui est de caractéristique 0). On pose pour tout k entre 1 et d, $\mathbb{L}_k = \mathbb{Q}(\alpha_k)$ et σ_k l'isomorphisme de $\mathbb{L}_1$ dans $\mathbb{L}_k$ qui envoie θ_1 sur θ_k. Puisque $\mathbb{K} = \mathbb{L}_1$, nous pouvons écrire

$$P(X_1, \ldots, X_n) = \sum_{l \in \mathbb{N}^n} c_l(\theta_1) X^l$$

où pour $l = (l_1, \ldots, l_n)$, $X^l = X^{l_1} \cdots X^{l_n}$ et $c_1 \in \mathbb{K}[T]$ est un polynôme de degré $< d$ (pour avoir unicité des coefficients). Pour tout $k = 1, \ldots, d$, notons

$$P^{(k)} = \sigma_k(P) = \sum_{l \in \mathbb{N}^n} c_l(\theta_k) X^l \in \mathbb{L}_1[X] \text{ et}$$
$$\overline{P} = P^{(1)} \cdots P^{(d)} \in \mathbb{L}[X_1, \ldots, X_n]$$

où $\mathbb{L}$ est de corps de décomposition de P_1 sur $\mathbb{Q}$. L'extension $\mathbb{L}$ est normale et séparable, il s'agit d'une extension galoisienne dont le groupe de Galois est $Gal = \{\sigma_1, \ldots, \sigma_d\}$. Mais alors, $\overline{P}$ est fixe sous l'action de Gal. Il s'ensuit que les coefficients de $\overline{P}$ sont dans $\mathbb{Q}$. Par ailleurs, $\deg(\overline{P}) = d\deg(P)$ comme souhaité. □

On dit que les nombres complexes $a_1, \ldots, a_t$ sont algébriquement indépendants, lorsque pour tout polynôme $P \in \mathbb{Q}[X_1, \ldots, X_t]$

$$P(a_1, \ldots, a_t) = 0 \Longrightarrow P = 0.$$

Cela générélise la notion d'indépendence linéaire (cas où P homogène est de degré 1). Dans ce cas, $\mathbb{T} = \mathbb{Q}[a_1, \ldots, a_t]$ est isomorphe à $\mathbb{Q}[X_1, \ldots, X_t]$.

Lemme 7.5 *Soit $a_1, \ldots, a_t$ des nombres complexes algébriquement indépendants, $\mathbb{T} = \mathbb{Q}[a_1, \ldots, a_t]$ et $\mathbb{E}$ une extension de degré d de $\mathbb{T}$. On pose $\mathbb{F} = \mathbb{E} \cap \overline{\mathbb{Q}}$ où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$. Alors $\mathbb{F}$ est une extension finie de $\mathbb{Q}$ de degré $\leq d$.*

Preuve : Soient $z_1, \ldots, z_{d+1}$ des eléments de $\mathbb{F}$, nous allons montrer que la famille $\{z_1, \ldots, z_{d+1}\}$ est $\mathbb{Q}$-liée. Comme $[\mathbb{E} : \mathbb{T}] = d$, on sait déjà que cette famille est $\mathbb{T}$-liée. Il existe des éléments $t_1, \ldots, t_{d+1}$ non nuls dans $\mathbb{T}$ tels que

$$\sum_{k=1}^{d+1} t_k z_k = 0.$$

Chaque éléments $t_k \in \mathbb{Q}[a_1, \ldots, a_t]$. En mulipliant par le ppcm de leur dénominateur, on obtient une famille $P_1, \ldots, P_{d+1}$ de polynômes de $\mathbb{Q}[a_1, \ldots, a_t]$ telle que

$$\sum_{k=1}^{d+1} P_k(a_1, \ldots, a_t) z_k = 0.$$

Posons

$$P = \sum_{k=1}^{d+1} P_k(X_1, \ldots, X_t) z_k \in \mathbb{Q}(z_1, \ldots, z_{d+1})[X_1, \ldots, X_t].$$

Comme les $z_1, \ldots, z_d$ sont algébriques, l'extension $\mathbb{K} = \mathbb{Q}(z_1, \ldots, z_{d+1})$ est finie de degré disons δ. De plus, $P(a_1, \ldots, a_t) = 0$. On peut donc appliquer le Lemme 7.4 pour obtenir un polynôme $\overline{P} \in \mathbb{Q}[X_1, \ldots, X_t]$ tel que $\overline{P}(a_1, \ldots, a_t) = 0$. Mais comme $a_1, \ldots, a_t$ sont algébriquement indépendants sur $\mathbb{Q}$, on a en fait $\overline{P} = 0$. Puisque $\deg(\overline{P}) = \delta \deg(P)$, on a aussi $P = 0$. Comme $P_k(X_1, \ldots, X_t)$ est dans $\mathbb{Q}[X_1, \ldots, X_t]$ et que $P_k(a_1, \ldots, a_t) = t_k \neq 0$, les P_k sont des polynômes non nuls à coefficients rationnels. Il existe donc $(x_1, \ldots, x_t) \in \mathbb{Q}^t$ tels que les $P_k(x_1, \ldots, x_t), k = 1, \ldots, d+1$ ne soient pas tous nuls. On a alors

$$\sum_{k=1}^{d+1} P_k(x_1, \ldots, x_t) z_k = 0$$

et les z_k sont liés dans $\mathbb{Q}$ comme souhaité. □

Soit N un entier naturel non nul. En reprenant les notations et hypothèses du lemme précédent, soit ξ une racine primitive N-ième de l'unité. On note R son polynôme minimal sur le corps $\mathbb{E}$ (ξ est algébrique sur $\mathbb{E}$ car il est algébrique sur $\mathbb{Q}$) et on pose $r = \deg(R)$.

Lemme 7.6 *Nous avons $\varphi(N) \leq dr$ où φ est l'indicatrice d'Euler sur les entiers.*

Preuve : Le polynôme $\mathbb{E}$ est à coefficients dans $\mathbb{F} = \mathbb{E} \cap \overline{\mathbb{Q}}$ puisqu'il divise $X^N - 1$. D'après le lemme 7.5, il existe donc un polynôme $\overline{R} \in \mathbb{Q}[X]$ tel que $\overline{R}\xi) = 0$ et $\deg(\overline{R}) = r[\mathbb{F} : \mathbb{Q}] \leq rd$. Par ailleurs Φ_N, le N-ième polynôme cyclotomique doit diviser $\overline{R}$ car $\overline{R} \in \mathbb{Q}[X]$ et Φ_N est irréductible sur $\mathbb{Q}$ avec $\Phi_N(\xi) = 0$. On a donc $\varphi(N) = \deg(\Phi_N) \leq rd$ comme souhaité. □

Théorème 7.7 (Schur) *Tout sous-groupe de $GL_n(\mathbb{C})$ de type fini et périodique est fini.*

Preuve : Soit G un sous-groupe de $GL_n(\mathbb{C})$ engendré par une partie $\mathcal{P}$ finie. On note $\mathbb{E}$ l'extension de $\mathbb{Q}$ enjendrée par les coefficients des matrices figurant dans $\mathcal{P}$. Comme ces coefficients sont en nombre fini, il existe une famille finie $\{a_1, \ldots, a_t\}$ d'éléments de $\mathbb{E}$ algébriquement indépendants tels que $\mathbb{E}$ soit une extension finie de $\mathbb{T} = \mathbb{Q}(a_1, \ldots, a_t)$ de degré d. Soit $A \in G$ et ξ une valeur propre de A. Comme A est d'ordre fini a, ξ doit être une racine de l'unité et donc une racine primitive pour un certain entier $N \leq a$. Par ailleurs, ξ est algébrique sur $\mathbb{E}$ car c'est une racine du polynôme caractéristique de A, matrice dont les coefficients sont dans $\mathbb{E}$ puisque A est un produit d'éléments de $\mathcal{P}$. Le lemme précédent montre donc que $\varphi(N) \leq dr$ où r est de degré de R le polynôme minimal de sur $\mathbb{E}$. Comme A est dans $GL_n(\mathbb{C})$, on a nécessairement $r \leq n$ et donc la majoration $\varphi(N) \leq dn$ où d et n sont des constantes indépendantes de A. D'après l'Exercice 7.8 nous avons donc $N \leq 6$ ou $N \leq d^2n^2$. Il existe donc une constante M telle que pour tout $A \in G$ et toute valeur propre ξ de A on ait $\Phi_N(\xi) = 0$ avec $N \leq M$. Les valeurs propres possibles des éléments de G sont donc en nombre fini et ce sont des racines de l'unité. En prenant par exemple le ppcm de tous les ordres possibles pour cet ensemble fini de racines de l'unité, on obtient donc une constante e telle que $\xi^e = 1$ pour toute valeur propre ξ de tout élément $A \in G$. Pour terminer, on remarque que chaque $A \in G$ est diagonalisable puisque $X^a - 1$ annule A et est scindé dans $\mathbb{C}$ à racines simples. Ainsi, $a \leq e$ et G est d'exposant fini. Il suffit donc d'appliquer le théorème de Burnside. □

7.4 Exercices

Exercice 7.8 *Montrer que la fonction d'Euler φ vérifie l'inégalité $\sqrt{n} \leq \varphi(n)$ pour tout entier $n \geq 7$.*

Exercice 7.9 *Soit G un groupe abelien d'exposant fini m et de type fini. Montrer que G est fini.*

Exercice 7.10 *Même question dans le cas d'un groupe abélien périodique et de type fini.*

Exercice 7.11 *Montrer qu'un groupe d'exposant 2 et de type fini est fini.*

Exercice 7.12 *Le but de l'exercice est de montrer que tout sous-groupe G de $GL_n(\mathbb{Q})$ de type fini et périodique est fini.sans bien sûr utiliser le théorème de Schur mais en admettant celui de Frobenius.*

1. *Soit $A \in G$ d'ordre m. Montrer que*

$$\ker P(A) = \bigoplus_{d/m} \ker \Phi_d(A)$$

   où Φ_d est le d-ième polynôme cyclotomique.
2. *Soit A_m la restriction de A à $V_m = \ker \Phi_m(A)$. Montrer que $\mu_{A_m} = \Phi_m$.*
3. *En déduire que l'ordre m d'un élément de G vérifie $\varphi(m) \leq n$ et conclure.*

Références

[1] Allesandrini. M, Thèmes de géométrie : groupe en situation, Dunod (1999).

[2] Beck. V., Malick. J, Peyré, G : Objectif agrégation, H&K (2005).

[3] Goblot. R, Algèbre Linéaire, Ellipse (2005).

[4] Gourdon. X, les maths en tête, Algèbre, Ellipse (1996).

[5] Grigorchuk. G, On the burnside problem on periodic groups, Funkts. Anal. Prilozen (1980).

[6] Perrin. D, Cours d'algèbre, Ellipse (1996).

[7] P. Samuel, Théorie des nombres. Hermann (1995).