ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Compléments d'algèbre linéaire

Benoit Loisel

25 septembre 2018

Leçons concernées (2018)

(150) Exemples d'actions de groupes sur les espaces de matrices.
(151) Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
(152) Déterminant. Exemples et applications.
(153) Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
(154) Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
(155) Endomorphismes diagonalisables en dimension finie.
(157) Endomorphismes trigonalisables. Endomorphismes nilpotents.
(159) Formes linéaires et dualité en dimension finie. Exemples et applications.
(162) Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Ce qui est dans le programme

(a) Espaces vectoriels, applications linéaires. Produit d'espaces vectoriels. Sous-espaces, image et noyau d'une application linéaire. Espaces quotients. Somme de sous-espaces, somme directe, supplémentaires. Familles libres, familles génératrices ; bases. Algèbre des endomorphismes d'un espace vectoriel E, groupe linéaire $\mathrm{GL}(E)$.

(b) Sous-espaces stables d'un endomorphisme. Valeurs propres, vecteurs propres, sous-espaces propres.

(c) Espaces vectoriels de dimension finie. Existence de bases : isomorphisme avec K^n. Existence de supplémentaires d'un sous-espace. Rang d'une application linéaire, rang d'un système de vecteurs. Espace dual. Rang d'un système d'équations linéaires. Transposée d'une application linéaire. Base duale. Bidualité. Orthogonalité.

(d) Applications multilinéaires. Déterminant d'un système de vecteurs, d'un endomorphisme. Groupe spécial linéaire $\mathrm{SL}(E)$. Orientation d'un $\mathbb{R}$-espace vectoriel.

(e) Matrices à coefficients dans un anneau commutatif. Opérations élémentaires sur les lignes et les colonnes, déterminant, inversibilité. Matrices à coefficients dans un corps. Rang d'une matrice. Représentations matricielles d'une application linéaire. Changement de base. Méthode du pivot de Gauss. Notion de matrices échelonnées. Applications à la résolution de systèmes d'équations linéaires, au calcul de déterminants, à l'inversion des matrices carrées, à la détermination du rang d'une matrice, à la détermination d'équations définissant un sous-espace vectoriel.

(f) Sous-espaces stables d'un endomorphisme, lemme des noyaux. Polynôme caractéristique. Polynômes d'endomorphismes. Polynômes annulateurs, polynôme minimal. Théorème de Cayley-Hamilton. Diagonalisation, trigonalisation. Sous-espaces caractéristiques, décomposition de Dunford. Exponentielle des matrices réelles ou complexes.

Bibliographie

- • marque les livres disponibles dans la bibliothèque de l'agreg ;
- $*$ marque les livres à ajouter absolument dans la malle si vous comptez les utiliser.

Cours

• J.-M. Arnaudiès et J. Bertin, *Groupes, algèbres et géométrie.* Ellipses, 1995.
Divers résultats d'algèbre.

• M. Artin, *Algebra.* Pearson Prentice Hall, 2011.
Si vous aimez montrer les muscles.

• G. Debeaumarché, *Manuel de mathématiques – Volume 4 Algèbre et géométrie – 2e année de prépas scientifiques MP-MP*.* Ellipses, 2006.
Pour les résultats élémentaires de L2.

* R. Goblot, *Algèbre linéaire.* Ellipses, 2005.
Algèbre linéaire sur les anneaux, $K[X]$-modules.

• X. Gourdon. *Algèbre.* Ellipse, 2009.
Un classique assez standard, niveau L2.

* J. Grifone. *Algèbre linéaire.* Cépaduès, 2011.
Un autre classique assez standard, niveau L3.

* R. Mansuy et R. Mneimné. *Algèbre linéaire. Réduction des endomorphismes.* Vuibert, 2012.
Une bonne référence de réduction.

• R. Mneimné, *Réduction des endomorphismes : tableaux de Young, cône nilpotent, représentations des algèbres de Lie semi-simples.* Calvage & Mounet, 2006.
Lire les introductions de chapitre pour enrichir sa culture générale.

• R. Mneimné et F. Testard, *Introduction à la théorie des groupes de Lie classiques.* Hermann, 1986.
Assez spécialisé, si vous voulez inclure des résultats spécifiques sur $\mathbb{R}$ ou $\mathbb{C}$. Attention, quelques coquilles peuvent s'y glisser : soyez vigilants !

* A. Paugam, *Agrégation de mathématiques – Questions délicates en algèbre et géométrie.* Dunod, 2007.
À lire à tête reposée pour consolider sa vision des choses.

• P. Tauvel. *Algèbre.* Dunod, 2005.
Un standard niveau L3.

Les mines d'exercices

• S. Francinou, H. Gianella et S. Nicolas. *Oraux X-Ens, algèbre 1.* Cassini, 2009.
* S. Francinou, H. Gianella et S. Nicolas. *Oraux X-Ens, algèbre 2.* Cassini, 2009.
* B. Hauchecorne, *Les contre-exemples en mathématiques.* Ellipses, 2007.
• P. Tauvel, *Exercices d'algèbre linéaire – 400 énoncés avec solutions détaillées.* Dunod, 2004.

1 Espaces quotients

Soit K un corps quelconque et E un K-espace vectoriel. Soit F un sous-espace vectoriel de E. On définit le quotient E/F comme suit :

(1) On définit sur E une relation d'équivalence par $x \sim y \Leftrightarrow \exists z \in F \quad y = x + z$

Exercice 1. Vérifier que c'est bien une relation d'équivalence.

(2) On définit l'ensemble E/F comme l'ensemble des classes d'équivalences pour $\sim$ et une application « quotient » $\begin{array}{cccc} \pi : & E & \to & E/F \\ & x & \mapsto & [x] \end{array}$ qui est surjective.

(3) On munit E/F d'une structure d'espace vectoriel par :

- $0_{E/F} = [0_E] = \pi(0_E)$;
- pour tous $\xi, \eta \in E/F$, si $x \in \xi$ et $y \in \eta$, on pose $\xi + \eta = [x + y]$ – cela ne dépend pas du choix de x et y ;
- pour tout $\xi \in E/F$, tout $\lambda \in K$, si $x \in \xi$, on pose $\lambda \cdot \xi = [\lambda x]$ – cela ne dépend pas du choix de $x \in \xi$ (exo).

Fait 1.1. *C'est l'unique structure de K-espace vectoriel sur E/F qui fasse de π une application K-linéaire.*

Remarque 1.2. Par construction, π est une application linéaire surjective de noyau F appelée **projection canonique de E sur F.**

Proposition 1.3 (Propriété universelle des quotients)**.** *Soit E, V des K-espaces vectoriels et F un sous-espace vectoriel de E. Si F est inclus dans* $\ker u$*, alors il existe une application linéaire $\overline{u} : E/F \to V$, unique, telle que u soit la composée de la projection canonique $E \to E/F$ et de $\overline{u}$.*

$$\begin{tikzcd} E \arrow[r, "u"] \arrow[d, "\pi"'] & V \\ E/F \arrow[ur, dashed, "\exists!\overline{u}"'] & \end{tikzcd}$$

Autrement dit, si $v \circ \pi = w \circ \pi$, alors $v = w$.

De plus, si $F = \ker u$, alors $\overline{u}$ est injective.

En particulier, $(E/F, \pi)$ est l'unique couple, à isomorphisme près, vérifiant cette propriété.

Démonstration. **Existence :** On prend $\xi \in E/F$ et $x \in \xi$. On pose $\overline{u}(\xi) = u(x)$. Cela ne dépend pas du choix de x. L'application ainsi définie $\overline{u}$ est K-linéaire.

Unicité : C'est la surjectivité de π.

Injectivité de $\overline{u}$: Si $\overline{u}(\xi) = 0$ et si $x \in \xi$, alors $u(x) = \overline{u}(\xi) = 0$. Ainsi $x \in \ker u$, donc $\xi = 0$.

Unicité de $(E/F, \pi)$: On applique la propriété universelle à un autre couple (V, u) et $\overline{u}$ donne l'isomorphisme. □

Exercice 2. Soient K un corps, E un K-espace vectoriel et F un sous-K-espace vectoriel. Soit $u : E \to V$ une application K-linéaire. On suppose que $F \subset \ker u$ et on note $\pi : E \to E/F$ la surjection canonique. Soit $\overline{u}$ une application linéaire telle que $u = \overline{u} \circ \pi$. Justifier que :

1. $\overline{u}$ est uniquement déterminée ;
2. $\overline{u}$ est injective si, et seulement si, $F = \ker u$;
3. $\overline{u}$ est surjective si, et seulement si, u l'est.

Théorème 1.4. *Si E est de dimension finie et si F est un sous-K-espace vectoriel de E, alors E/F est de dimension*

$$\dim(E/F) = \dim(E) - \dim(F)$$

Démonstration. Il n'est a priori pas évident que E/F est de dimension finie. π est une application linéaire surjective donc l'image d'une famille génératrice finie est une famille génératrice finie de E/F. En particulier, E/F est de dimension finie.

Notons $r = \dim F$ et $s = \dim E/F$. Soit $(f_1, \ldots, f_r)$ une base de F et $(\xi_1, \ldots, \xi_s)$ une base de E/F. On choisit $e_1, \ldots, e_s \in E$ tels que $e_i \in \xi_i$. Alors $(e_1, \ldots, e_s, f_1, \ldots, f_r)$ est une base de E. En effet, c'est :
- une famille libre car si $\sum \lambda_i e_i + \sum \mu_j f_j = 0$, alors en appliquant $\pi : E \to E/F$, on a $\sum \lambda_i \xi_i = 0$ donc pour tout i, on a $\lambda_i = 0$. Ainsi $\sum \mu_j f_j = 0$ donc pour tout j, on a $\mu_j = 0$.
- une famille génératrice car si $x \in E$, alors il existe des $\lambda_i \in K$ tels que $\pi(x) = \sum \lambda_i \xi_i$. Donc $x - \sum \lambda_i e_i \in F$. Ainsi, il existe des μ_j tels que $x - \sum \lambda_i e_i = \sum \mu_j f_j$. □

2 Dualité

Soit K un corps et E un K-espace vectoriel.

Définition 2.1. On appelle **espace dual** et on note $E^* = \mathrm{Hom}(E, K)$ l'espace des formes linéaires sur E. L'espace dual de l'espace dual, appelé **bidual**, est noté E^{**}.

Soit E un K-espace vectoriel admettant une base $(e_i)_{i\in I}$. Pour tout $i \in I$, on peut définir une application linéaire e_i^* uniquement déterminée par les formules :

$$e_i^*(e_j) = 0 \text{ si } j \neq i \quad \text{et} \quad e_i^*(e_i) = 1$$

Fait 2.2. *La famille $(e_i^*)_{i\in I}$ est libre.*

Démonstration. On raisonne sur l'ensemble des parties finies $J \subset I$. Il suffit d'évaluer toute combinaison linéaire $\sum \lambda_j e_j^*$ sur la famille libre des $(e_j)_{j\in J}$. □

Exemple 2.3. En dimension infinie, cette famille n'est pas génératrice. Prenons par exemple $E = K[X]$ l'espace vectoriel des polynômes avec pour base les monôme unitaires $(X^i)_{i\in\mathbb{N}}$. Quelle est la famille duale (f_i) associée ? Pourquoi ne peut-on pas écrire $\begin{array}{ccc} K[X] & \to & K \\ P & \mapsto & P(1) \end{array}$ comme combinaison linéaire (finie) d'éléments de (f_i) ?

Théorème 2.4. *Si E est de dimension finie, alors E^* aussi et* $\dim(E) = \dim(E^*)$.

Démonstration. Si $(e_1, \ldots, e_n)$ est une base de E, alors on a vu que $(e_1^*, \ldots, e_n^*)$ est une famille libre de E^*. C'est aussi une famille génératrice car pour tout $f \in E^*$, on a :

$$f = \sum_{i=1}^{n} f(e_i) e_i^*$$

□

Définition 2.5. On définit **l'application canonique de E dans son bidual** $\begin{array}{cccc} \iota : & E & \to & E^{**} \\ & x & \mapsto & \widehat{x} \end{array}$ qui à un vecteur $x \in E$ associe l'évaluation $\begin{array}{cccc} \widehat{x} : & E^* & \to & K \\ & f & \mapsto & f(x) \end{array}$ en x.

Proposition 2.6. *(1) L'application canonique de E dans son bidual est linéaire et injective.*
(2) Si E est de dimension fini, alors ι est un isomorphisme canonique entre E et E^{**}.

Démonstration. (1) Il est facile de voir que i est linéaire (exo).

Pour montrer que ι est injective, admettons l'existence de bases en toute dimension (en acceptant par exemple l'axiome du choix) *. Soit $x \in E \setminus \{0\}$. Si on complète x en une base, alors on peut définir $x^* \in E^*$ telle que $x^*(x) = 1 \neq 0$. En particulier $\widehat{x} \neq 0$.

(2) Si E est de dimension finie, alors ι est une application linéaire injective entre espaces de même dimension. □

Corollaire 2.7. *Si E est de dimension finie, alors on a une bijection naturelle de l'ensemble des bases de E sur l'ensemble des bases de E^* :*

$$\Psi : (e_1, \ldots, e_n) \mapsto (e_1^*, \ldots, e_n^*)$$

Démonstration. **Injectivité :** si $(e_1, \ldots, e_n)$ et $(e'_1, \ldots, e'_n)$ ont même base duale $(f_1, \ldots, f_n)$, alors pour tout $1 \leq i, j \leq n$, on aurait $f_j(e_i - e'_i) = 0$. Donc $e_i - e'_i \in (F^*)^\top = \{x \in E \ , \ \forall f \in F^* \quad f(x) = 0\}$ où $F = \mathrm{Vect}(f_1, \ldots, f_n)$. Or $F = E$ car (f_i) est une base (dimension finie) et $(E^*)^\top = \{0\}$ par (2). D'où $e_i = e'_i$ pour tout i.

Surjectivité : Soit $(f_1, \ldots, f_n)$ une base de E^* et $(f_1^*, \ldots, f_n^*)$ la base duale associée dans E^{**}. On considère l'isomorphisme canonique $\iota : E \to E^{**}$ et on pose $e_i = \iota^{-1}(f_i^*)$ pour tout $i \in [\![1, n]\!]$. Alors $(e_1, \ldots, e_n)$ est une base de E car ι est un isomorphisme et pour tous $i, j \in [\![1, n]\!]$, on a $f_j(e_i) = \psi(e_i)(f_j) = f_i^*(f_j) = \delta_{i,j}$. Ainsi, on retrouve bien la formule des f_j définissant la base duale de e_i. □

*. Je ne connais pas d'autre preuve que celle-ci.

3 Transposition et orthogonalité

Définition 3.1. Soit V et W deux espaces vectoriels, et $f \in \mathrm{Hom}_K(V, W)$. On note f^t l'élément de $\mathrm{Hom}_K(W^*, V^*)$ donné par $f^t(\lambda) = \lambda \circ f$. On l'appelle **la transposée** de f.

Remarque 3.2. On le note aussi parfois f^*.

Fait 3.3. *Soit $u \in \mathrm{Hom}_K(V, W)$. Si on se donne des bases de V et W, alors la matrice de la transposée dans les bases duales associées est la transposée de la matrce de*

Démonstration. Ceci est laissé en exercice au lecteur. □

Remarque 3.4. Attention : on prendra soin de ne pas confondre la notion d'orthogonalité induite par la dualité de celle d'orthogonalité définie dans le cadre des formes bilinéaires et quadratiques, bien qu'un lien naturel existe entre les deux. Plus précisément, ce lien est donné par le choix d'un isomorphisme (non canonique) entre E et E^* qui fait de la forme bilinéaire suivante :

$$\begin{array}{ccc} E \times E^* & \to & K \\ (x, g) & \mapsto & \langle x, f\rangle := f(x) \end{array}$$

une forme symétrique définie positive.

Définition 3.5. Soit E un K-espace vectoriel. Soit X une partie de E. On appelle **orthogonal** de X, noté $X^\perp$, l'ensemble des formes linéaires $f \in E^*$ telles que pour tout $x \in X$, on a $f(x) = \langle x, f\rangle = 0$. Soit Y une partie de E^*. On appelle **orthogonal** de Y, noté $Y^\top$, l'ensemble des vecteurs $x \in E$ tels que pour tout $f \in Y$, on a $f(x) = \langle x, f\rangle = 0$.

Les propriétés élémentaires de l'orthogonalité et ses liens avec la transpositions seront vues en exercice.

Lemme 3.6. *Soit E un K-espace vectoriel et F, G deux sous-espaces vectoriels tels que $E = F \oplus G$. Soit $j : F \hookrightarrow E$ l'inclusion. Alors sa transposée $j^t : E^* \to F^*$ est surjective de noyau* $\ker j^t = F^\perp \simeq G^*$.

Démonstration. Soit $v \in F^* = \mathrm{Hom}_K(F, K)$. Soit $\pi_F : E \to F$ la projection sur F parallèlement à G. On peut étendre v en une forme linéaire $u = v \circ \pi_F \in E^*$. Par définition, $j^t(u) = u \circ j = v$. En particulier, on obtient la surjectivité de j^t.

Soit $u \in E^*$ que l'on écrit $u = v + w$ avec $v = u_{|F} \in F^*$ et $w = u_{|G} \in G^*$. Pour que u soit dans $\ker j^t$, il faut, et il suffit, que $0 = j^t(u) = v$. Ainsi $\ker j^t$ est l'espace des formes linéaires sur E qui s'annulent sur F, c'est-à-dire $F^\perp$.

Soit π_G la projection sur G parallèlement à F. Alors l'application $w \mapsto w \circ \pi_G$ réalise un isomorphisme entre G^* et $F^\perp$. □

Théorème 3.7. *Soit E un K-espace vectoriel de dimension finie, F un sous-espace vectoriel de E et F' un sous-espace vectoriel de E^*. On a les égalités* $\dim F + \dim F^\perp = \dim E = \dim F' + \dim F'^\top$.

Démonstration. Par le lemme, comme j^t est surjective de noyau $F^\perp$, on a l'isomorphisme $\mathrm{im}\, j^t = F^* \simeq E^*/F^\perp$. Donc $\dim F^* = \dim E^* - \dim F^\perp$. On conclut en utilisant $\dim E = \dim E^*$ et $\dim F = \dim F^*$.

Soit $(f_1, \ldots, f_m)$ une base de F' que l'on complète en une base $(f_1, \ldots, f_n)$ de E^*. Soit $(e_1, \ldots, e_n)$ la base antéduale de $(f_1, \ldots, f_n)$. Alors, on a $F'^\top = \mathrm{Vect}(e_{p+1}, \ldots, e_n)$. D'où le résultat. □

Remarque 3.8. Soit E un espace vectoriel de dimension finie n et F un sous-espace vectoriel de dimension m. On a donc $\dim F^\perp = n - m = r$. Soit $(\lambda_1, \ldots, \lambda_s)$ un système de générateurs de $F^\perp$. On a nécessairement $s \geq r$ et $F = F^{\perp\top}$. Ainsi $x \in F \Leftrightarrow \lambda_i(x) = 0\ \forall i \in [\![1, r]\!]$. Les relations $\lambda_i(x) = 0$ constituent un système d'équations du sous-espace F et on peut s'arranger pour en choisir exactement la codimension de F, à savoir $r = \mathrm{codim}\, F = \dim E - \dim F = \dim F^\perp$.

Réciproquement, soit $(\lambda_1, \ldots, \lambda_s)$ un système de rang r d'éléments non nuls de E^*. Le système d'équations $\lambda_i(x) = 0$ caractérise le sous-espace vectoriel $F = \mathrm{Vect}(\lambda_1, \ldots, \lambda_s)^\top$ et on a $\dim F = n - r$. Si on extrait de $(\lambda_1, \ldots, \lambda_s)$ une base $(\mu_1, \ldots, \mu_r)$ de $\mathrm{Vect}(\lambda_1, \ldots, \lambda_s)$ et si on pose $H_i = \ker \mu_i$, alors on obtient $F = \bigcap H_i$. Ainsi, un sous-espace vectoriel de codimension r est l'intersection de r hyperplans.

4 Invariants de similitude

L'esprit de la réduction des endomorphismes est de pouvoir choisir une base dans laquelle les calculs sont facilités. À ce titre, on aimerait trouver, si possible, une base dans laquelle la matrice d'un endomorphisme est diagonale ou, à défaut, triangulaire supérieur. Ceci est toujours possible sur un corps algébriquement clos mais ce n'est plus le cas sur un corps quelconque.

Un changement de base revient à effectuer l'opération matricielle $A' = P^{-1}AP$ où P est une matrice de passage. On est en fait en train de regarder l'action du groupe $\mathrm{GL}_n(K)$ sur l'espace vectoriel des matrices carrées $\mathcal{M}_n(K)$ par conjugaison $P \cdot A = P^{-1}AP$. Les orbites de cette action sont appelées classes de similitude Trouver une forme « plus simple » d'une matrice A à similitude près c'est choisir un « bon » représentant de l'orbite de A. L'un des objets de la réduction est donc de choisir des représentants et de décrire les classes de similitude pour ces éléments. On parlera alors de matrices diagonalisables et trigonalisables.

On voudrait également disposer d'un algorithme qui décide si deux matrices sont semblables ou non, autrement dit, on cherche un système d'invariants complet pour cette action. Vous connaissez des invariants à similitude près, par exemple le rang, la trace, le déterminant, le polynôme caractéristique, le polynôme minimal. En général, ces invariants ne suffisent pas à distinguer les classes de similitude.

Avant de parler des facteurs invariants d'une matrice, rappelons quelques résultats sur les polynômes d'endomorphisme. Les démonstrations vous sont laissées en exercices, ce sont des rappels de prépa.

Dans toute la suite, K désigne un corps quelconque et E un K-espace vectoriel de dimension finie. Si $u \in \mathrm{End}(E)$, et $\lambda \in K$, on note

- $E'_u(\lambda) = \bigcup_{k \geq 0} \ker(u - \lambda\,\mathrm{id})^k$ le **sous-espace caractéristique** associé à λ et
- $E_u(\lambda) = \ker(u - \lambda\,\mathrm{id})$ le **sous-espace propre** associé à λ.

Polynômes d'endomorphismes

Par la propriété universelle des anneaux de polynômes, il existe un unique morphisme de K-algèbres :

$$\begin{array}{ccc} K[X] & \to & \mathrm{End}(E) \\ P = \sum_{k=0}^{n} \lambda_k X^k & \mapsto & \sum_{k=0}^{n} a_k \underbrace{u \circ \cdots \circ u}_{k-\text{fois}} \end{array}$$

Son image est une K-algèbre, notée $K[u]$ et son noyau est un idéal strict de $K[X]$. Comme $K[X]$ est principal, il est engendré par un élément μ_u, qu'on peut supposer unitaire, appelé **polynôme minimal** de u.

Fait 4.1. *Tout polynôme annulant u est divisible par μ_u.*

On note également $\chi_u = \det(X\,\mathrm{id} - u)$ le **polynôme caractéristique** de u.

Remarque 4.2. On remarquera également que ceci définit une structure de $K[X]$-module sur E, notée E_u, par $P \cdot x = P(u)(x)$. On identifie alors les sous-espaces stables par u aux sous-$K[X]$-modules de E_u.

Définition 4.3. On dit que λ est une **valeur propre** si les conditions équivalentes suivantes sont vérifiées :

(i) $\chi_u(\lambda) = 0$;
(ii) $\mu_u(\lambda) = 0$;
(iii) $E_u(\lambda) \neq \{0\}$;
(iv) $E'_u(\lambda) \neq \{0\}$.

Proposition 4.4 (Lemme des noyaux)**.**
Soit $Q = Q_1 \dots Q_r$ un produit de polynômes deux à deux premiers entre eux.

Alors $\ker Q(u) = \bigoplus_{k=1}^{r} \ker Q_k(u)$.

Théorème 4.5 (Cayley-Hamilton)**.**
On a $\chi_u(u) = 0$.

Proposition 4.6 (Critère de diagonalisabilité).
S'équivalent :

(i) u *est* diagonalisable*, c'est-à-dire qu'il existe une base de* E *dans laquelle la matrice de* u *est diagonale ;*

(ii) u *est annulé par un polynôme scindé à racines simples ;*

(iii) μ_u *est scindé à racines simples ;*

(iv) E *admet une base formée de vecteurs propres pour* u *;*

(v) $E = \oplus_\lambda E_u(\lambda)$.

Proposition 4.7 (Critère de trigonalisation).
S'équivalent :

(i) u *est* trigonalisable*, c'est-à-dire qu'il existe une base de* E *dans laquelle la matrice de* u *est triangulaire supérieure ;*

(ii) u *est annulé par un polynôme scindé ;*

(iii) μ_u *est scindé ;*

(iv) χ_u *est scindé ;*

(v) $E = \oplus_\lambda E'_u(\lambda)$.

Théorème 4.8 (Décomposition de Dunford).
On suppose χ_u *scindé. Alors il existe un unique couple d'endomorphismes* (d, n) *tels que :*
- d *est diagonalisable,*
- n *est nilpotent,*
- $u = d + n$,
- d *et* n *commutent.*

De plus, d *et* n *sont des polynômes en* u.

Invariants de similitude

Définition 4.9. Un sous-espace F de E est dit u**-monogène** (on dit aussi que u est F**-cyclique**), s'il existe $x \in F$ tel que $\mathrm{Vect}(u^k(x),\ k \in \mathbb{N}) = F$.

Fait 4.10. *Si* F *est* u*-monogène, alors* F *est* u*-stable et il existe une base de* F *dans laquelle la matrice de* $v = u_{|F}$ *est la matrice compagnon du polynôme* $\mu_v = X^d + c_{d-1}X^{d-1} + \cdots + c_0$*, à savoir*

$$\begin{pmatrix} 0 & \dots & \dots & 0 & -c_{d-1} \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -c_0 \end{pmatrix}.$$

Démonstration. Soit $d = \dim(F)$. Par définition, il existe $x \in F$ tel que la famille $(v^k(x))_{k\in\mathbb{N}}$ engendre F. Comme $\chi_v(v)(x) = v^d(x) + \cdots + \det(-v)x = 0$, on en déduit que la famille $(x, \dots, v^{d-1}(x))$ engendre F, donc que c'en est une base pour des raisons de cardinalité. En particulier, c'est une famille libre donc $\deg \mu_{v,x} = d$. Comme $\mu_{v,x} | \mu_v$, on a $\deg \mu_v$ et la forme souhaitée de la matrice de v dans la base indiquée. $\square$

On dira également que u est **cyclique** si E est u-monogène.

Le but de cette section est de donner une démonstration n'utilisant pas le point de vue moderne des $K[X]$-modules du théorème suivant :

Théorème 4.11. *Il existe une décomposition* $E = \bigoplus_{k=1}^{r} F_k$ *en sous-espaces* F_k*, qui sont* u*-monogènes, telle que la suite des polynômes* $P_k = \mu_{u_{|F_k}}$ *est décroissante pour l'ordre de la division des polynômes, c'est-à-dire que* $P_r | \dots | P_1$.

De plus, une telle suite de polynômes est uniquement déterminée par u.

Remarque 4.12. On remarque immédiatement que $P_1 = \mu_u$ et $\prod_i P_i = \chi_u$. En effet, pour tout i, on a $\chi_{u_{|F_i}} = \mu_{u_{|F_i}}$ car F est u-monogène.

De plus, les P_i sont invariants par similitude car si $v = gug^{-1}$, alors la famille des $g(F_i)$ est v-monogène et fournit les mêmes polynômes.

Définition 4.13. Les polynômes P_i sont appelés **facteurs invariants** de u.

On notera $\mu_{u,x}$ un générateur unitaire de l'idéal $\{P \in K[X],\ P(u)(x) = 0\}$.

Lemme 4.14. *Soit* $x_1, \dots, x_m \in E$ *et* $x = \sum_{k=1}^m x_k$. *Soit* $F_k = \{P(u)(x_k),\ P \in K[X]\}$. *Si les* F_k *sont en somme directe, alors* $\mu_{u,x} = \mathrm{ppcm}(\mu_{u,x_1}, \dots, \mu_{u_{x_m}})$.

Démonstration. Soit $P = \mathrm{ppcm}(\mu_{u,x_1}, \dots, \mu_{u,x_m})$. Comme $\mu_u(u)(x_k) = 0$, on a $P(u)(x_k) = 0$ pour tout k. Ainsi $P(u)(x) = 0$.

D'autre part, en posant $y_k = \mu_{u,x}(u)(x_k) \in F_k$, on a $\mu_{u,x}(u)(x) = 0 = \sum_{k=1}^m y_k$. Donc $y_k = 0$ pour tout k. Ainsi $\mu_{u,x_k} | \mu_{u,x}$ donc $P | \mu_{u,x}$. ☐

Proposition 4.15. *Il existe* $x \in E$ *tel que* $\mu_u = \mu_{u,x}$.

Démonstration. On décompose μ_u en puissances de facteurs irréductibles unitaires $P_k^{a_k}$ deux à deux premiers entre eux. Par le lemme des noyaux, on a $E = \bigoplus_k \ker P_k^{a_k}(u)$. Pour tout k, on choisit $x_k \in \ker P_k^{a_k}(u) \setminus \ker P_k^{a_k - 1}(u)$. Ceci est possible car sinon le polynôme μ_u / P_k annulerait encore u.

On a alors $F_k = \{P(u)(x_k),\ P \in K[X]\} \subset \ker P_k^{a_k}(u)$ et les F_k sont en somme directe. De plus $\mu_{u,x_k} = P_k^{a_k}$ car P_k est irréductible et $P_k^{a_k}(u)(x) = 0$. Par le lemme précédent, on obtient ainsi que $\mu_{u,x} = \mathrm{ppcm}(\mu_{u,x_k}) = \prod P_k^{a_k} = \mu_u$. ☐

On peut désormais démontrer le théorème.

Démonstration du théorème sur les facteurs invariants.
Existence : On procède par récurrence sur $\dim E = n$. Si $n \leq 1$, il n'y a rien à démontrer. Sinon, soit $x \in E$ tel que $\mu_u = \mu_{u,x}$ et $d = \deg(\mu_u)$. Par définition, la famille $(e_1, \dots, e_d) = (x, u(x), \dots, u^{d-1}(x))$ est libre. On pose $F = \mathrm{Vect}(e_1, \dots, e_d)$. Si $F = E$, on a terminé. Sinon, on va construire un supplémentaire u-stable de F.

Complétons $(e_1, \dots, e_d)$ en une base $(e_1, \dots, e_n)$ de E et considérons sa base duale $(e_1^*, \dots, e_n^*)$ dans E^*. Soit $\Gamma = \left\{(u^k)^t(e_d^*),\ k \in \mathbb{N}\right\}$ et $G = \Gamma^\top$ l'orthogonal de Γ. Par construction G est u-stable. Montrons que G est un supplémentaire de F dans E :

- Si par l'absurde, il existait $y \in F \cap G \setminus \{0\}$, alors on pourrait écrire $y = \lambda_1 e_1 + \cdots + \lambda_s e_s$ avec $s \leq d$ et $\lambda_s \neq 0$. Mais alors $0 = (u^{d-s})^t(e_d^*)(y) = e_d^*(\lambda_1 e_{d-s} + \cdots + \lambda_s e_d) = \lambda_s$ est une contradiction. Ainsi $F \cap G = \{0\}$.
- On a $\dim \mathrm{Vect}(\Gamma) = d = \dim F$ car l'application :

$$\begin{array}{ccc} K[u] & \to & \mathrm{Vect}(\Gamma) \\ P(u) & \mapsto & P(u)^t(e_d^*) \end{array}$$

  est un isomorphisme. Ainsi $\dim \Gamma^\top = \dim E - \dim F$.

Considérons $v = u_{|G}$ et posons $P_1 = \mu_u$ et $P_2 = \mu_v$. On a alors $P_2 | P_1$ et on conclut par hypothèse de récurrence appliquée à (v, G).
Unicité : Soit $E = F_1 \oplus \cdots \oplus F_r = G_1 \oplus \cdots \oplus G_s$ deux suites de décomposition vérifiant les hypothèses du théorème. Notons $(P_r | \dots | P_1)$ et $(Q_s | \dots | Q_1)$ leurs suites de polynômes associées. Supposons par l'absurde que ces suites sont distinctes. Soit $j = \min\{i \in \mathbb{N},\ P_i \neq Q_i\}$, ce qui existe car $\sum_i \deg P_i = \sum_i \deg Q_i = n$. Comme $\mu_u = P_1 = Q_1$, on a $j \geq 2$. De plus, on a :

$$P_j(u)(E) = P_j(u)(F_1) \oplus \cdots \oplus P_j(u)(F_{j-1}) = P_j(u)(G_1) \oplus \cdots \oplus P_j(u)(G_s)$$

Les sommes sont en effet directes car les F_i, G_i sont $P_j(u)$ stables. Pour $i < j$, on a $\dim P_j(u)(F_i) = \dim P_j(u)(G_i)$ car $u_{|F_i}$ et $u_{|G_i}$ sont semblables à une même matrice compagnon $C(P_i) = C(Q_i)$. Ainsi, pour tout $i \geq j$, on a $P_j(u)(G_i) = 0$. Donc $Q_j | P_j$. Par symétrie, on a aussi $P_j | Q_j$ en échangeant les rôles des F_i et G_i. D'où $P_j = Q_j$, ce qui contredit la définition de j. D'où l'unicité de la suite des facteurs invariants. ☐

Exercice 3. Calculer les facteurs invariants :
– d'une homothétie ;
– d'un endomorphisme diagonalisable ayant toutes ses valeurs propres distinctes ;
– d'une transvection ;
– d'un endomorphisme nilpotent (discuter suivant son ordre) ;
– d'un projecteur (discuter suivant sa trace).

Applications

Il reste à montrer que la famille des facteurs invariants constituent bien un invariant complet pour l'action de $\mathrm{GL}_n(K)$ sur $\mathcal{M}_n(K)$ par conjugaison.

Théorème 4.16 (Décomposition de Frobenius)**.** *Soit $(P_r|\dots|P_1)$ la suite des invariants de similitude de $u \in \mathrm{End}(E)$. Il existe une base de E dans laquelle u a pour matrice*

$$\begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_n) \end{pmatrix}$$

Démonstration. Soit $E = F_1 \oplus \cdots \oplus F_r$ une décomposition associée aux facteurs invariants $P_r|\dots|P_1$. Pour tout i, il existe une base de F_i dans laquelle $u_{|F_i}$ est semblable à $C(P_i)$ car F_i est$u_{|F_i}$-monogène par construction. Leur réunion donne une base convenable dans E. □

Corollaire 4.17. *Deux matrices sont semblables si, et seulement si, leurs facteurs invariants sont égaux.*

Exercice 4. Soit L/K une extension de corps Montrer que deux matrices de $\mathcal{M}_n(K)$ sont semblables sur L si, et seulement si, elles sont semblables sur K.

Jordanisation

Un corollaire élémentaire de la réduction de Frobenius est la décomposition de Jordan, qui donne alors, pour un endomorphisme, une forme efficace pour effectuer des calculs (exponentielle par exemple), à condition d'en être capable de calculer le changement de base. Théoriquement, l'intérêt est au moins de pouvoir donner une esquisse locale du diagramme de phase d'une EDL par exemple.

Définition 4.18. On appelle **bloc de Jordan** de taille r de paramètre λ la matrice

$$J_r(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix} \in \mathcal{M}_r(K)$$

Par exemple $J_1(\lambda) = (\lambda)$.

Théorème 4.19 (Décomposition de Jordan)**.** *Soit $u \in \mathrm{End}(E)$ un endomorphisme trigonalisable. Alors il existe une base de E et des paramètres $(r_i, \lambda_i) \in \mathbb{N}^* \times K$ tels que la matrice de u dans cette base est diagonale par blocs de Jordan de paramètres (r_i, λ_i),*

$$\begin{pmatrix} J_{r_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{r_s}(\lambda_s) \end{pmatrix}$$

Démonstration. Notons $d = \dim E$. Traitons d'abord le cas d'un endomorphisme nilpotent $n \in \mathrm{End}(E)$. Soit $P_r|\dots|P_1$ ses invariants de similitude. Par nilpotence, $\mu_n = P_1$ divise X^d donc, pour tout $1 \leq i \leq r$, on a $C(P_i) = J_{\deg P_i}(0)^t$. Par la décomposition de Frobenius, on peut trouver une base de E dans laquelle la matrice de n s'écrit :

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

Quitte à conjuguer par la matrice de permutation P_σ pour $\sigma = (d\ \ldots\ 2\ 1)$, on obtient une matrice de la forme

$$\operatorname{Mat}_{\mathcal{B}}(n) = \begin{pmatrix} J_{r_1}(0) & & 0 \\ & \ddots & \\ 0 & & J_{r_s}(0) \end{pmatrix}$$

Revenons maintenant au cas général et décomposons $E = \bigoplus E'_u(\lambda)$ en somme directe de ses sous-espaces caractéristiques, qui sont u-stables. Alors sur chaque $F = E'_u(\lambda)$, l'endomorphisme $v = u_F - \lambda \operatorname{id}_F$ est nilpotent. Il existe donc une base $\mathcal{B}_\lambda$ de F dans laquelle on peut jordaniser v. Dans cette base, la matrice de $\lambda \operatorname{id}_F$ est scalaire, de paramètre λ. Donc

$$\operatorname{Mat}_{\mathcal{B}_\lambda}(u_{E'_u(\lambda)}) = \begin{pmatrix} J_{r_{1,\lambda}}(\lambda) & & 0 \\ & \ddots & \\ 0 & & J_{r_{s_\lambda,\lambda}}(\lambda) \end{pmatrix}$$

On choisit alors la base $\mathcal{B} = \bigsqcup_\lambda \mathcal{B}_\lambda$ qui convient. □

Commutant

Donnons une autre application des invariants de similitudes On appelle *commutant* d'un endomorphisme $u \in operatornameEnd(E)$, la K-algèbre $\operatorname{Comm}(u) = \{v \in \operatorname{End}(E),\ [u,v] = u \circ v - v \circ u = 0\}$ des endomorphismes qui commutent à u. Il est clair que $K[u] \subset \operatorname{Comm}(u)$ en est une sous-K-algèbre.

Théorème 4.20. *On a l'équivalence*

$$K[u] = \operatorname{Comm}(u) \qquad \Longleftrightarrow \qquad u \text{ est cyclique.}$$

Démonstration. Supposons que $K[u] = \operatorname{Comm}(u)$. Par le théorème 4.11, on peut trouver une décomposition de E en sous-espaces F_k qui sont u-monogènes. Soit q la projection sur $\bigoplus_{i=2}^r F_i$ parallèlement à F_1. Alors q commute à u car les F_i sont u-stables. Donc q est un polynôme en u, disons $q = Q(u)$ avec $Q \in K[X]$. On a $0 = Q(u)_{F_1} = Q(u_{F_1})$. Donc $P_1 = \mu_{u_{F_1}} = \mu_u$ divise Q. Or, les facteurs invariants étant des diviseurs de P_1, on a que $P_i = \mu_{u_{F_i}} | Q$. En particulier $0 = Q(u_{F_i}) = q_{F_i}$. On trouve alors que $E = F_1$, ce qui signifie que u est cyclique.

Réciproquement, si u est cyclique, alors il existe un $x \in E$ tel que $E = K[u] \cdot x$. Si v commute à u, alors $v(x) = P(u)(x)$. Donc, pour tout $y = Q(u)(x) \in E = K[u] \cdot x$, on a bien $v(y) = v(Q(u)(x) = Q(u)(v(x)) = Q(u)P(u)(x) = P(u)Q(u)(x) = P(u)(y)$. Ce qui prouve que $\operatorname{Comm}(u) \subset K[u]$. □