Algèbre linéaire : rappels et compléments

« En inventant l'arme prestigieuse qui porte son nom, Césarien de la Baïonette a plus fait pour la guerre que Sœur Teresa pour les pauvres » – P. Desproges

Table des matières

Avant de reprendre la théorie de première année et la compléter, quelques mots sur **le pivot de Gauss**, qui est l'outil effectif principal en algèbre linéaire. Il est omniprésent dans les différents calculs que vous devez savoir faire :

- Pour résoudre un système linéaire, on pivote [1] : c'est quasiment le seul moment en mathématiques où travailler par équivalence est pertinent, possible et facile. Plus on veut finasser et « gagner du temps » avec je ne sais quelles astuces ou « méthodes » prébac, et plus on perd du temps et on se trompe. C'est ainsi. Accessoirement, le pivot vous assure une description du sous-espace affine des solutions à l'aide d'une base.
- Pour calculer un rang, on pivote sur les lignes jusqu'à arriver à une matrice de la forme

$$\begin{pmatrix} T & \vdots & M \\ \cdots & \cdots & \cdots \\ 0_{n-r,r} & \vdots & 0_{n-r,p-r} \end{pmatrix},$$

  avec $T \in \mathcal{M}_r(\mathbb{K})$ triangulaire à coefficients diagonaux non nuls : le rang de T – mais aussi et surtout de la matrice initiale – est alors r.
- Pour calculer un déterminant, on fait des opérations sur les lignes et colonnes (pour faire apparaître des zéros) avant de développer selon une ligne ou colonne, etc : c'est du pivot !
- Pour inverser une matrice, on peut selon contexte : calculer une matrice de passage inverse (c'est du pivot) ou résoudre formellement $AX = Y$ (c'est du pivot) ou encore travailler formellement sur une matrice initialement égale à I_n, qui se transforme miraculeusement en A^{-1} si on réalise sur elle les opérations conduisant A à I_n : encore du pivot.
- Pour calculer P et Q inversibles telles que $PAQ = J_r$ (avec r le rang de A), il est conseillé de raisonner géométriquement... mais les experts peuvent pivoter formellement pour obtenir le résultat.
- Pour extraire d'une famille une base de l'espace engendré, et la compléter en une base de l'espace ambiant... on représente les vecteurs en question dans une base *qui ne bougera pas*, et on pivote sur les colonnes...

1 Géométrie des espaces vectoriels

1.1 Rappels sur les (sous-)espaces, bases...

La définition d'un espace vectoriel vous sera à peu près aussi utile que celle d'une série. C'est dire...

Définition 1 — *Espaces ; sous-espaces ; combinaisons linéaires*

Soit $\mathbb{K}$ un corps (concrètement, et pour rester dans le programme : $\mathbb{R}$ ou $\mathbb{C}$).

- Un **$\mathbb{K}$-espace vectoriel** est un ensemble E muni d'une loi de composition interne $+$ et d'une loi de composition externe $\mathbb{K} \times E \to E$ telles que $(E, +)$ est un groupe commutatif, de neutre noté $\overrightarrow{0_E}$, « la loi externe et la loi interne se comportant honorablement l'une vis-à-vis de l'autre ».
- Une **combinaison linéaire** d'éléments de E est un vecteur de la forme $\lambda_1\overrightarrow{x_1}+\cdots+\lambda_n\overrightarrow{x_n}$, avec les λ_i dans $\mathbb{K}$ (« scalaires ») et les $\overrightarrow{x_i}$ dans E (« vecteurs »).
- Un **sous-espace vectoriel** d'un espace E est une partie non vide stable par combinaisons linéaires.

Exemples :

- $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel. On peut voir $\mathbb{C}^n$ comme un $\mathbb{C}$-espace vectoriel mais aussi un $\mathbb{R}$-espace vectoriel (et la dimension change alors).
- $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.
- $\mathcal{C}^\infty(I)$ est un sous-espace de $\mathcal{C}^1(I)$, qui est lui-même un sous-espace de $\mathcal{D}^1(I)$, qui est lui-même... etc.
- L'ensemble $\mathcal{S}_n(\mathbb{K})$ des matrices (n, n) symétriques constitue un sous-espace de $\mathcal{M}_n(\mathbb{K})$.

1. À titre exceptionnel, les champions des cramerisations sont autorisés à jouer en dimension 2, pour peu qu'ils ne fassent pas n'importe quoi, hypothèse très optimiste...

— L'ensemble des suites complexes vérifiant la relation $f_{n+2} = f_n + f_{n+1}$ est un sous-espace de l'espace $\mathbb{C}^{\mathbb{N}}$ des suites complexes.
— Si $u \in \mathcal{L}(E)$, l'ensemble des endomorphismes de E commutant avec u est un sous-espace de $\mathcal{L}(E)$.
— Si $x_1, ..., x_n \in E$, l'ensemble des combinaisons linéaires des x_i est un sous-espace de E, noté $\text{Vect}(x_1, ..., x_n)$. C'est même le plus petit sous-espace de E contenant les x_i : on parle de **sous-espace engendré par les** x_i, et la définition reste la même pour une famille infinie $(x_i)_{i\in I}$.

Remarques :
— Si F est un sous-espace de E, il hérite naturellement de la structure d'espace vectoriel (et partage le même neutre pour l'addition).
— Les sous-espaces sont souvent présentés sous forme duale : ils peuvent être vus comme des noyaux, ou comme des ensembles de combinaisons linéaires. Passer d'une représentation à l'autre fait partie des activités de base en algèbre linéaire :

$$\{(x,y,z) \in \mathbb{R}^3;\ x+y+z=0\} = \{(-\alpha-\beta, \alpha, \beta) \,|\, \alpha,\beta \in \mathbb{R}\} = \{\alpha\overrightarrow{u} + \beta\overrightarrow{v} \,|\, \alpha,\beta \in \mathbb{R}\} = \text{Vect}(\overrightarrow{u}, \overrightarrow{v}),$$

avec $\overrightarrow{u} = (-1,1,0)$ et $\overrightarrow{v} = (-1,0,1)$.
— Les combinaisons linéaires sont toujours des sommes *finies*. Même quand on parle d'une combinaison linéaire d'un ensemble *infini* de vecteurs, comme $(X^n)_{n\in\mathbb{N}}$ par exemple, très différente de $(X^i)_{0\leqslant i\leqslant n}$.

Définition 2 — *Familles libres, génératrices*

Une famille $(\overrightarrow{v_i})_{i\in I}$ de vecteurs de E est :
— **génératrice** lorsque tout vecteur $\overrightarrow{f}$ de E est combinaison linéaire des $\overrightarrow{v_i}$ (i.e. : il existe $\lambda_1, ..., \lambda_n \in \mathbb{K}$, $i_1, ..., i_n \in I$ tels que $\overrightarrow{f} = \lambda_1\overrightarrow{v_{i_1}} + \cdots + \lambda_n\overrightarrow{v_{i_n}}$).
— **libre**, ou **linéairement indépendante**, lorsque la seule combinaison linéaire nulle des $\overrightarrow{v_i}$ est la combinaison linéaire triviale. Autrement dit : si $\lambda_1\overrightarrow{v_{i_1}} + \cdots + \lambda_n\overrightarrow{v_{i_n}} = \overrightarrow{0}$, alors tous les λ_i sont nuls. Dans le cas contraire (existence d'une combinaison linéaire nulle et non triviale), on dit que la famille est **liée** (implicitement : « liée par une relation de dépendance linéaire »).
— **une base** lorsque tout vecteur de E s'écrit de façon unique comme combinaison linéaire des $\overrightarrow{v_i}$.

Remarques :
— On montre facilement qu'une famille est une base si et seulement si elle est libre et génératrice (le faire tout de même : il y a une équivalence à prouver !)
— Dans le cas où $I = \{1, 2, ..., n\}$, ces notions peuvent se reformuler en termes de surjectivité/injectivité de l'application

$$\Phi \left\| \begin{array}{ccc} \mathbb{K}^n & \longrightarrow & E \\ (\lambda_1, ..., \lambda_n) & \longmapsto & \lambda_1\overrightarrow{v_1} + \cdots + \lambda_n\overrightarrow{v_n} \end{array} \right.$$

Exemples :
— Pour deux vecteurs : (v_1, v_2) est liée si et seulement si ces deux vecteurs sont colinéaires : il existe λ tel que $v_1 = \lambda v_2$ ou $v_2 = \lambda v_1$ (attention, ce n'est pas la même chose : le premier cas ne couvre pas celui où $v_1 \neq 0$ et $v_2 = 0$).
— De même pour n vecteurs, une famille est liée si et seulement si l'un des vecteurs est combinaison linéaire des autres : vérifiez-le !
— Dans $\mathbb{K}^n$, on connaît la « base canonique » $\mathcal{E} = (e_1, ..., e_n)$ avec $e_i = (0, ..., 0, 1, 0, ..., 0)$, mais il y en a bien d'autres...
— Dans $\mathbb{K}_n[X]$, on dispose encore d'une base privilégiée (la « base canonique » $(1, X, ..., X^n)$). Dans $\mathbb{K}[X]$, $(X^n)_{n\in\mathbb{N}}$ est une bien plus grosse base !
— Dans $\mathcal{M}_{n,p}(\mathbb{K})$, la famille constituée des $E_{i,j}$ (matrice (n,p) dont le coefficient en position (k,ℓ) vaut 1 si $(i,j) = (k,\ell)$ et 0 sinon. Bref : $(E_{i,j})_{k,\ell} = \delta_{i,k}\delta_{j,\ell}$!) constitue une base naturelle souvent appelée « base canonique ».
— En dehors des trois cas vus plus haut, point de base canonique. Vous ne parlerez donc JAMAIS de la base canonique d'un espace E quelconque.
— Non mais vraiment, en fait !
— Les suites géométriques $(\varphi_1^n)_{n\in\mathbb{N}}$ et $(\varphi_2^n)_{n\in\mathbb{N}}$ (avec φ_1 et φ_2 les deux racines de $X^2 - X - 1$) constituent une base de l'espace des suites « de type Fibonacci » (vérifiant $u_{n+2} = u_n + u_{n+1}$ pour tout $n \in \mathbb{N}$, sans conditions initiales imposées).
— On se souvient qu'en dimension finie égale à n, les familles libres ont un cardinal **majoré** par n, et les génératrices ont leur cardinal **minoré** par n (on reviendra dessus bientôt).

Exemples : *En dimension infinie*

— Dans $\mathbb{K}[X]$, les familles échelonnées en degré (familles $(P_n)_{n\in\mathbb{N}}$ avec P_n de degré n pour tout $n \in \mathbb{N}$) constituent DES bases. Si on impose juste aux degrés d'être différents, on trouve des familles libres (mais plus forcément génératrices : penser à $(X^{2n})_{n\in\mathbb{N}}$).

— Dans $\mathcal{C}^0(\mathbb{R})$, la famille constituée des $f_n : x \mapsto |x-n|$ est libre mais non génératrice. Même chose dans $\mathcal{C}^\infty(\mathbb{R})$ pour la famille constituée des $\varphi_n : x \mapsto \mathrm{e}^{inx}$.

— Dans $\mathbb{K}(X)$, la famille constituée des $\dfrac{1}{X-\alpha}$ (avec α décrivant $\mathbb{K}$) est libre non génératrice.

Exercice 1. *Dans* $\mathbb{R}^3$*, on définit* $v_1 = \begin{pmatrix}1\\2\\3\end{pmatrix}$ *(abus de notation pour parler de* $(1,2,3)$*),* $v_2 = \begin{pmatrix}2\\1\\1\end{pmatrix}$ *et* $v_3 = \begin{pmatrix}-1\\4\\7\end{pmatrix}$*. Montrer que la famille* $\mathcal{F} = (v_1, v_2, v_3)$ *est liée. En extraire une base de* $\mathrm{Vect}(\mathcal{F})$*, et compléter la famille ainsi obtenue pour en faire une base de* $\mathbb{R}^3$*.*

Remarque : En dimension finie, l'existence d'une base sera assurée (soit dans la définition, soit comme conséquence de la définition). En dimension infinie, c'est plus délicat : on considère des « familles libres maximales » pour avoir l'existence de bases. Cette notion de « maximale » nécessite quelques précautions logiques sur lesquelles nous passerons pudiquement.

1.2 Rappels sur les applications linéaires

Définition 3 — *Applications linéaires*

Une application f de E dans F est dite **linéaire** lorsque :

$$\forall x, y \in E, \quad \forall \alpha, \beta \in \mathbb{K}, \qquad f(\alpha x + \beta y) = \alpha f(x) + \beta f(y).$$

L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}(E,F)$. C'est clairement (?) un $\mathbb{K}$-espace vectoriel.

Exemples :

— $(x,y,z) \in \mathbb{R}^3 \mapsto (x+y+z, 2x-z) \in \mathbb{R}^2$; $(x_1,...,x_n) \in \mathbb{R}^n \mapsto \sum_{i=1}^{n} i x_i \in \mathbb{R}$.

— $P \in \mathbb{K}[X] \mapsto XP' \in \mathbb{K}[X]$; $P \in \mathbb{R}[X] \mapsto \displaystyle\int_{972}^{999} P(t)dt \in \mathbb{R}$.

— $M \in \mathcal{M}_n(\mathbb{K}) \mapsto M + \mathrm{tr}(M) I_n \in \mathcal{M}_n(\mathbb{K})$; $M \in \mathcal{M}_n(\mathbb{K}) \mapsto \mathrm{tr}(AM) \in \mathbb{K}$.

— $f \in \mathcal{C}^\infty(I) \mapsto f'' + 2f' + f \in \mathcal{C}^\infty(I)$.

Proposition 1 — Images directes et réciproques de sous-espaces

Si $u \in \mathcal{L}(E,F)$, avec E_1 un sous-espace de E et F_1 un sous-espace de F, alors $u(E_1)$ est un sous-espace de F, et $u^{<-1>}(F_1)$ est un sous-espace de E.

Preuve : À savoir faire ! C'est en particulier l'occasion de réapprendre (ou d'apprendre) à manipuler des images réciproques : u n'est pas supposée bijective, et $u^{<-1>}(F_1)$ n'est donc pas « l'ensemble des ... avec ... décrivant ... » mais plutôt « l'ensemble des ... tels que ... » ■

Dans la proposition précédente, on obtient une information « assez faible » lorsque $E_1 = \{0\}$ ou $F_1 = F$. Ce n'est pas exactement la même chose si on prend les deux autres sous-espaces triviaux auxquels on peut penser.

Définition 4 — *Noyau, image d'une application linéaire*

Soit $u \in \mathcal{L}(E,F)$. Son **noyau** est l'ensemble des antécédents de 0_F par u :

$$\mathrm{Ker}\,(u) := u^{<-1>}(\{0_F\}) = \{x \in E \ ; \ u(x) = 0_F\}$$

et son **image** est :

$$\mathrm{Im}\,(u) := u(E) = \{u(x) \mid x \in E\}.$$

Ce sont des sous-espaces de respectivement E et F.

On aura noté que $\mathrm{Ker}\,(u)$ est « l'ensemble des ... tels que ... » alors que $\mathrm{Im}\,(u)$ est « l'ensemble des ..., avec ... décrivant ... ». Tant que vous ne saurez pas **lire** les choses correctement, vous galérerez...

Exemples :

- L'ensemble $\{(\alpha, \beta, 2\beta-\alpha) \,|\, \alpha, \beta \in \mathbb{R}\}$ peut être vu à la fois comme le noyau de $(x, y, z) \mapsto x-2y+z$, l'image de $(\alpha, \beta) \mapsto (\alpha, \beta, 2\beta - \alpha)$, ou encore l'espace engendré par $(1, 0, -1)$ et $(0, 1, 2)$.
- Les matrices de trace nulle constituent le noyau d'une application linéaire [2] !
- Les suites « de type Fibonacci » peuvent être vues comme le noyau de l'application qui à une suite u associe la suite v définie par $v_n = u_{n+2} - u_n - u_{n+1}$ pour tout $n \in \mathbb{N}$.

Par définition des deux notions (surjectivité et image), une application linéaire est surjective si et seulement si son image est égale à l'ensemble d'arrivée ; ceci n'apporte pas grand chose... C'est une autre affaire pour l'injectivité ! Certes, si une application linéaire est injective, alors $\{0\}$ possède au plus un antécédent, puis exactement un antécédent, donc son noyau est réduit au neutre de l'espace de départ. Mais la réciproque, bien que simple, apporte vraiment quelque chose !

Théorème 1 — *Caractérisation de l'injectivité*

Une application $u \in \mathcal{L}(E, F)$ est injective si et seulement si son noyau est réduit à $\{0_E\}$.

Exemples :

- L'application $(a, b) \in \mathbb{R}^2 \mapsto (a + b, a + 2b, 2a + b, a + 3b) \in \mathbb{R}^4$ est injective.
- Par contre, l'application $(a, b, c, d) \in \mathbb{R}^4 \mapsto (a + b + c + d, a - b + c - d) \in \mathbb{R}^2$ n'est pas injective (on s'en serait douté au vu des dimensions, non ?)
- L'application $P \in \mathbb{R}_n[X] \mapsto (P(1), P(2), ..., P(n + 1)) \in \mathbb{R}^{n+1}$ est injective.
- Enfin, si $\mathcal{E}$ est une base de E, alors $u \in \mathcal{L}(E) \mapsto \mathrm{Mat}(u, \mathcal{E}) \in \mathcal{M}_n(\mathbb{K})$ est injective.

Exercice 2. *Les applications précédentes sont-elles surjectives ?*

Les résultats suivants doivent devenir naturels... et dans un premier temps il faut être capable de les prouver sans trembler, puis à encéphalogramme plat.

Exercice 3. *Soit $u \in \mathcal{L}(E, F)$*

1. *Montrer que si u est injective, alors l'image par u d'une famille libre de E est toujours une famille libre de F.*
2. *Donner un contre-exemple sans l'hypothèse d'injectivité.*
3. *Montrer que si $(u(v_1), ..., u(v_n))$ est libre dans F, alors $(v_1, ..., v_n)$ est libre dans E.*
4. *Montrer que si u est surjective et $(v_1, ..., v_n)$ est génératrice dans E, alors $(u(v_1), ..., u(v_n))$ est une famille génératrice de F.*
5. *Que dire de l'image d'une base par u, lorsque u est bijective ?*

On prouve sans mal que la composée d'applications linéaires est linéaire, et que si $u \in \mathcal{L}(E, F)$ est bijective, alors sa bijection réciproque u^{-1} est linéaire (écrire la preuve tout de même).

Définition 5 — *Certaines applications linéaires : du vocabulaire*

Si E est un espace vectoriel, $\mathcal{L}(E, E)$ est noté $\mathcal{L}(E)$: ses habitants (applications linéaires de E dans lui-même) sont appelés **endomorphismes** de E. $(\mathcal{L}(E), +, ., \circ)$ est alors une algèbre.
Les applications linéaires qui sont bijectives sont appelées des **isomorphismes**. Les endomorphismes qui sont également des isomorphismes sont appelés des **automorphismes** : leur ensemble constitue le **groupe linéaire**, et... c'est un groupe pour la loi $\circ$ (ouf).

Terminons par un certain nombre de résultats laissés en exercice, mais leur preuve doit être quasiment instantanée, et ils devront être connus assez rapidement :

Exercice 4. *Soient $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$. Montrer :*

1. $\mathrm{Ker}\,(u) \subset \mathrm{Ker}\,(v \circ u)$ *et* $\mathrm{Im}\,(v \circ u) \subset \mathrm{Im}\,(v)$.
2. $v \circ u = 0$ *si et seulement si* $\mathrm{Im}\,(u) \subset \mathrm{Ker}\,(v)$.
3. *Si $E = F$ et $u \circ v = v \circ u$, alors l'image et le noyau de u sont stables par v.*

2. Sauras-tu trouver celle à laquelle je pense ?

1.3 « Interpolation linéaire »

Attention, ce terme d'« interpolation linéaire » n'est pas standard ! Il s'agit juste de faire le rapprochement avec un autre théorème qui nous dit qu'on peut trouver une application (polynomiale) envoyant des points donnés sur des images imposées (vu en première année, et rappelé en dernière partie de ce chapitre).

THÉORÈME 2 — *Interpolation linéaire – a.k.a. : construction d'une application linéaire par l'image d'une base.*

> Si $(e_1, ..., e_n)$ est une base de E et $f_1, ..., f_n \in F$, alors il existe une unique application linéaire $u \in \mathcal{L}(E, F)$ telle que pour tout $i \in [\![1, n]\!]$, $u(e_i) = f_i$.

PREUVE : Analyse-synthèse : l'analyse nous dit quelle est la seule façon envisageable de définir $u(x)$. Dans la synthèse, on vérifie qu'en définissant ainsi u, on obtient bien une application linéaire répondant au cahier des charges. ■

REMARQUES :
- Quand on parle de « l'application linéaire envoyant telle base sur telle famille », on utilise implicitement le résultat précédent.
- De même, définir une application linéaire par sa matrice entre deux bases (« soit u l'application linéaire dont la matrice entre telles bases vaut ceci ») revient implicitement à utiliser ce résultat.
- On dispose donc (en attendant la suite !) de trois façons de définir une application linéaire : de façon directe (avec une formule explicite), en imposant l'image d'une base, ou en imposant sa matrice entre deux bases.

Exercice 5. *Soient F et G deux sous-espaces de E de dimension finie. Donner une condition nécessaire et suffisante sur F et G pour qu'il existe $u \in \mathcal{L}(E)$ tel que $\mathrm{Im}\,(u) = F$ et $\mathrm{Ker}\,(u) = G$.*

SOLUTION : La condition « F et G sont supplémentaires » est raisonnable : en tout cas *suffisante* (penser alors à la projection de F parallèlement à G), mais pas *nécessaire* : prendre $E = \mathbb{R}_2[X]$, $F = \mathbb{R}_1[X]$ et $G = \mathbb{R}_0[X]$: F et G sont l'image et le noyau de l'application $P \mapsto P'$ sans être supplémentaires.
Le théorème du rang nous donne une autre condition (*nécessaire*, cette fois) : $\dim(F)+\dim(G) = \dim(E)$.
Pour montrer qu'elle est *suffisante*, on la suppose vérifiée. On considère une base $(g_1, ..., g_k)$ de G qu'on complète en une base de E, on considère une base $(f_1, ..., f_{n-k})$ de F qu'on complète en une base de E, et on considère enfin l'unique application linéaire envoyant les f_i sur... ce qu'il faut pour que ça marche [3] !

1.4 Aspects dimensionnels

Un espace est déclaré **de dimension finie** lorsqu'il possède une famille génératrice finie. On souhaite alors montrer qu'il possède une base finie, et que toutes les bases possèdent le même nombre d'éléments. On a pour cela besoin des résultats classiques qui suivent :

THÉORÈME 3 — *Extraction, complétion*

> Les familles considérées ici sont indexées par des ensembles finis I ou J. On note E l'espace ambiant.
> - Si $(e_i)_{i\in I}$ est une famille génératrice de E, alors on peut en extraire une base $(e_k)_{k\in K}$.
> - Si $\mathcal{E} = (e_i)_{i\in I}$ est libre et $\mathcal{F} = (f_j)_{j\in J}$ est génératrice, alors on peut compléter $\mathcal{E}$ avec une sous-famille de $\mathcal{F}$ pour en faire une base de E.

PREUVE : Pour l'extraction, on considère une sous-famille libre de cardinal maximal : elle constitue une base de E. On aurait également pu considérer une sous-famille génératrice de cardinal minimal : elle est libre.
Pour la complétion, c'est encore un argument de famille « intermédiaire » génératrice minimale ou libre maximale. ■

REMARQUE : En dimension infinie, on dispose de résultats de même nature, mais pour la preuve, on a besoin d'une notion de « famille maximale » assez naturelle, mais qui requiert quelques précautions de logiciens.

THÉORÈME 4 — *Libre vs générateur : size* does *matter !*

> S'il existe dans un espace une famille génératrice de cardinal n, alors toute famille de cardinal $n + 1$ est liée.

PREUVE : Récurrence sur n, via un coup de pivot. ■

3. Left to the reader.

Ainsi, si un espace possède deux bases finies alors elles ont le même cardinal (ne pas passer trop vite sur ce point important : en détailler la preuve).

DÉFINITION 6 — *Dimension d'un espace*

Si un espace est de dimension finie, **sa dimension** est le cardinal commun de toutes ses bases.

D'après ce qui précède, en dimension n, les familles libres (respectivement génératrices) sont de cardinal majoré (respectivement minoré) par n.

EXEMPLES :

- $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel de dimension n. *Attention,* $\mathbb{C}^n$ *est un* $\mathbb{C}$*-espace vectoriel de dimension* n*, mais un* $\mathbb{R}$*-espace vectoriel de dimension* $2n$*.*
- $\mathbb{K}_n[X]$ est de dimension... tadam.... $n+1$, merci.
- Si E et F sont de dimension finie, alors $\mathcal{L}(E,F)$ aussi, avec $\dim(\mathcal{L}(E,F)) = \dim(E)\dim(F)$.
- $\mathcal{M}_{n,p}(\mathbb{K})$ est de dimension np.

Le résultat suivant (Grassmann [4], 1844) est important... et l'esprit de sa preuve aussi (construire des bases adaptées aux différents sous-espaces en jeu).

THÉORÈME 5 — *Grassmann*

Si E_1 et E_2 sont deux sous-espaces vectoriels de E de dimension finie, alors :

$$\dim(E_1+E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2).$$

PREUVE : Créer une base de E_1+E_2 adaptée à tous les sous-espaces en jeu... en *commençant* par l'intersection. ■

Dans le même esprit (au niveau de la preuve), on pourra traiter l'exercice suivant :

Exercice 6. *Soient* E_1 *et* E_2 *deux sous-espaces de* E *de dimension finie, avec* $\dim(E_1) = \dim(E_2)$*. Montrer que* E_1 *et* E_2 *possèdent un supplémentaire commun.*

L'exercice suivant est très simple via Grassmann...

Exercice 7. *Déterminer la dimension de l'intersection de deux hyperplans distincts d'un espace de dimension finie.*

Notons dès maintenant qu'il ne peut pas se passer n'importe quoi entre des espaces de dimension finie (et la formule du rang précisera cela)...

Exercice 8. *Soient* E *et* F *de dimension finie. Montrer que s'il existe une application linéaire injective (respectivement surjective) de* E *dans* F*, alors* $\dim(E) \leqslant \dim(F)$ *(respectivement :* $\dim(E) \geqslant \dim(F)$*).*

Le théorème suivant regroupe quatre résultats typiques de la dimension finie, tous dans le même esprit.

THÉORÈME 6 — *Principes linéaires de fainéantise*

1. Soit E un espace de dimension finie égale à n. Pour une famille de n vecteurs de E, il y a équivalence entre le fait d'être une base, d'être libre ou d'être générateur.
2. Soient E_1 et E_2 deux sous-espaces de E de dimension finie tels que $\dim(E_1)+\dim(E_2) = \dim(E)$. Il y a alors équivalence entre : « E_1 et E_2 sont supplémentaires », « $E_1 \cap E_2 = \{0_E\}$ », et « $E_1 + E_2 = E$ ».
3. Soient E et F deux espaces de dimensions finies et égales et $u \in \mathcal{L}(E,F)$. Il y a alors équivalence entre la bijectivité, l'injectivité et la surjectivité de u.
4. Si deux (sous-)espaces sont de même dimension, alors l'inclusion de l'un dans l'autre est équivalente à leur égalité.

PREUVE : À savoir faire les yeux fermés ! Pour le dernier résultat, on peut se passer du « théorème du rang ». ■

4. Pour les connaisseurs : « La formule ? » « Ben ouais, j'en connais pas dix, hein ».

1.5 Noyaux et images itérés, endomorphismes nilpotents

Si $u \in \mathcal{L}(E)$, on note en général $u^k = \underbrace{u \circ u \circ \cdots \circ u}_{k \text{ fois}} \in \mathcal{L}(E)$. On vérifie alors sans mal [5] les inclusions :

$$\cdots \subset \mathrm{Im}\,(u^{n+1}) \subset \mathrm{Im}\,(u^n) \subset \cdots \subset \mathrm{Im}\,(u^2) \subset \mathrm{Im}\,(u) \subset \mathrm{Im}\,(u^0) = \mathrm{Im}\,(\mathrm{Id}_E) = E$$

et aussi :

$$\{0_E\} = \mathrm{Ker}\,(\mathrm{Id}_E) = \mathrm{Ker}\,(u^0) \subset \mathrm{Ker}\,(u) \subset \mathrm{Ker}\,(u^2) \subset \cdots \subset \mathrm{Ker}\,(u^n) \subset \mathrm{Ker}\,(u^{n+1}) \subset \cdots$$

Remarque : En dimension finie, les dimensions sont donc des suites d'entiers croissantes majorées ou décroissantes minorées, donc vont stationner. On a même mieux ; patience !

Exemples :

- Pour les projections et symétries, ça stationne vite...
- Si u est l'endomorphisme « dérivation » dans $\mathbb{K}_n[X]$, il y a des inclusions strictes pour les images et noyaux, jusqu'au rang $n+1$ à partir duquel ça stagne. Mais si on voit u comme un endomorphisme de $\mathbb{K}[X]$, il y a des inclusions strictes pour les noyaux, mais la suite des images itérées est constante.
- On pourra également observer $u : P \in \mathbb{K}[X] \mapsto XP$: left to the reader.

Le résultat qui suit n'est pas difficile à montrer, mais est moins direct, tout en restant important :

Proposition 2 — Stagnation des images et noyaux itérés

Si $\mathrm{Ker}\,(u^{n_0}) = \mathrm{Ker}\,(u^{n_0+1})$, alors $\mathrm{Ker}\,(u^{n_0}) = \mathrm{Ker}\,(u^n)$ pour tout $n \geqslant n_0$. De même, Si $\mathrm{Im}\,(u^{n_0}) = \mathrm{Im}\,(u^{n_0+1})$, alors $\mathrm{Im}\,(u^{n_0}) = \mathrm{Im}\,(u^n)$ pour tout $n \geqslant n_0$.

Preuve : On suppose $\mathrm{Ker}\,(u^{n_0}) = \mathrm{Ker}\,(u^{n_0+1})$, et on prouve $\mathrm{Ker}\,(u^{n_0+1}) = \mathrm{Ker}\,(u^{n_0+2})$ (pour l'inclusion non triviale, on fixe $x \in \mathrm{Ker}\,(u^{n_0+2})$: on a alors $u(x) \in \mathrm{Ker}\,(u^{n_0+1})$, donc $u(x) \in \mathrm{Ker}\,(u^{n_0})$, etc...). On conclut par récurrence. Même chose pour les images. ■

Exercice 9. *Déterminer les noyaux et images de u^k, pour $k \in \mathbb{N}$, avec u l'endomorphisme de $\mathbb{R}^6$ canoniquement associé à*

$$\begin{pmatrix} 2 & 1 & & & & \\ 0 & 2 & & & & \\ & & 0 & 1 & & \\ & & 0 & 0 & & \\ & & & & 0 & \\ & & & & & 42 \end{pmatrix}$$

(il y a des zéros partout ailleurs).

On passe maintenant à quelques propriétés des endomorphismes nilpotents.

Définition 7 — *Nilpotence*

Un endomorphisme de E est dit **nilpotent** lorsqu'il existe $k \in \mathbb{N}$ tel que $u^k = 0$. Lorsque c'est le cas, le plus petit indice k tel que $u^k = 0$ est appelé l'**indice de nilpotence** de u.

Remarque : Attention, si u est la dérivation dans $E = \mathbb{K}[X]$, alors pour tout $P \in E$, il existe $k \in \mathbb{N}$ tel que $u^k(P) = 0$, et pourtant il n'existe pas de $k \in \mathbb{N}$ tel que pour tout $P \in E$, $u^k(P) = 0$: la dérivation n'est pas nilpotente sur $\mathbb{K}[X]$ (mais elle l'est sur $\mathbb{K}_n[X]$).

Exercice 10. *Soit u un endomorphisme nilpotent de E de dimension n. Montrer que $u^n = 0$.*

Solution : On peut le prouver en utilisant les résultats précédents sur les noyaux itérés : tant que ça ne stagne pas, la dimension des noyaux augmente d'au moins un, et cette dimension est majorée par la dimension de l'espace...
Autre façon de le faire (plus directe) : on note p l'indice de nilpotence. Il existe alors x_0 tel que $u^{p-1}(x_0) \neq 0$, et on prouve alors que la famille $\big(x_0, u(x_0), ..., u^{p-1}(x_0)\big)$ est libre. Comme elle est de cardinal p...
Ainsi, l'indice de nilpotence est majoré par la dimension de l'espace.

5. Oui, on le fait quand même !

Exercice 11. *CCINP 2010 (PC)*
Soit $f \in \mathcal{L}(\mathbb{C}^n)$ telle que $f^{n-1} \neq 0$ et $f^n = 0$. Montrer qu'il existe une base de $\mathbb{C}^n$ dans laquelle la matrice M de f vérifie $M_{i,j} = \begin{cases} 1 & \text{si } j = i+1 \\ 0 & \text{sinon} \end{cases}$

Si la matrice d'un endomorphisme dans une base donnée est triangulaire supérieure stricte (des zéros sur la diagonale), on voit sans trop de mal que l'endomorphisme est nilpotent (à chaque puissance supplémentaire, il apparaît une nouvelle « diagonale » de zéros). La réciproque est vraie !

PROPOSITION 3 — Les nilpotents sont trigonalisables

> En dimension finie, si un endomorphisme est nilpotent, alors il existe une base dans laquelle la matrice de cet endomorphisme est triangulaire supérieure.

PREUVE : Observer les inclusions strictes :

$$\operatorname{Ker}(u) \subsetneq \operatorname{Ker}(u^2) \subsetneq \cdots \subsetneq \operatorname{Ker}(u^{p-1}) \subsetneq \operatorname{Ker}(u^p) = E,$$

et construire une base de l'espace en commençant par une base de $\operatorname{Ker}(u)$, complétée en une base de $\operatorname{Ker}(u^2)$, complétée...
Quelle est alors la matrice de u dans une telle base ? Il n'y a plus grand chose à faire...
On peut même affiner un peu[6] *la preuve en imposant seulement quelques* 1 *dans cette matrice, avec des zéros partout ailleurs. Mais c'est une autre histoire (« réduction de Jordan »).* ■

Exercice 12. *CCINP 2009 (PSI)*
Soient E un $\mathbb{C}$-espace vectoriel de dimension trois, et $f \in \mathcal{L}(E)$. Montrer : $\operatorname{Im}(f^3) = \operatorname{Im}(f^4)$.

1.6 Sommes directes (au delà de deux sous-espaces...)

RAPPEL : si E_1 et E_2 sont deux sous-espaces de E, il y a équivalence (à savoir prouver) entre :
- tout vecteur de E se décompose de façon unique comme somme d'un élément de E_1 et un élément de E_2 ;
- $E_1 \cap E_2 = \{0\}$ (« E_1 et E_2 sont en somme directe ») et $E_1 + E_2 = E$.

Les sous-espaces E_1 et E_2 sont alors déclarés *supplémentaires*. En dimension finie, tout sous-espace possède un (en fait, *des*) supplémentaire(s) : complétion de bases. Le résultat reste vrai en dimension infinie, toujours avec les précautions de logiciens.

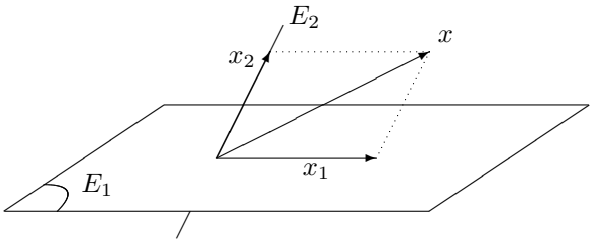


FIGURE 1 – $x \in E_1 + E_2$ mais $x \notin E_1 \cup E_2$

Exercice 13. *Montrer que toute application de $\mathbb{R}$ dans $\mathbb{R}$ se décompose de façon unique comme somme d'une fonction paire et d'une fonction impaire.*

REMARQUE : Ainsi, les sous-espaces $\mathcal{P}$ et $\mathcal{I}$ constitués des fonctions paires (respectivement impaires) sont supplémentaires dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$. On notera que la preuve par analyse-synthèse est essentiellement la même que celle nous assurant que tout endomorphisme u de E vérifiant $u \circ u = \mathrm{Id}_E$ est une symétrie, avec en particulier $\operatorname{Ker}(u - \mathrm{Id}_E)$ et $\operatorname{Ker}(u + \mathrm{Id}_E)$ supplémentaires. Ce n'est (peut-être) pas un hasard...

6. Beaucoup en fait ! Prendre une base d'un supplémentaire de $\operatorname{Ker}(u^{p-1})$; son image par u constitue une famille libre de $\operatorname{Ker}(u^{p-2})$: on la complète en une base de $\operatorname{Ker}(u^{p-2})$; l'image par u de cette base est alors une famille libre de...

Définition 8 — *Sous-espaces en somme directe*

Soit E un espace vectoriel, et $E_1, ..., E_n$ des sous-espaces de E. Ces sous-espaces sont déclarés **en somme directe** lorsque tout vecteur de $E_1 + \cdots + E_n$ se décompose de façon unique sous la forme $v_1 + \cdots + v_n$, avec $v_i \in E_i$. On note alors la somme $E_1 \oplus \cdots \oplus E_n = \bigoplus_{k=1}^{n} E_k$.

Remarques :

- Pour être en somme directe, la condition $E_i \cap E_j = \{0_E\}$ pour $i \neq j$ reste nécessaire (unicité de la décomposition de 0_E) mais n'est plus suffisante : penser à trois droites distinctes dans $\mathbb{R}^2$. En fait, une condition nécessaire et suffisante consiste à imposer à chaque E_i d'avoir une intersection triviale avec la somme des E_j, pour $j \neq i$: c'est inutilisable en pratique, donc oubliez cette bêtise (si vous l'avez rencontrée) !
- Si on recolle des bases de sous-espaces en somme directe, alors on trouve une base de la somme. Réciproquement, si on casse une base de l'espace en différents morceaux, les sous-espaces engendrés sont en somme directe, et leur somme vaut tout l'espace.
- Dans le cas de la dimension finie, la dimension d'une somme directe est égale à la somme des dimensions des sous-espaces en jeu (voir la remarque précédente).

Proposition 4 — Une caractérisation efficace des sommes directes

Si $E_1, ..., E_n$ sont des sous-espaces de E, alors ils sont en somme directe si et seulement si la seule décomposition du vecteur nul selon cette somme est la décomposition triviale.

Proposition 5 — Dimension d'une somme

Soient $E_1, E_2, ..., E_k$ des sous-espaces de E, espace de dimension finie. Alors :

- $\dim(E_1 + \cdots + E_k) \leqslant \dim(E_1) + \cdots + \dim(E_k)$;
- si la somme est directe, alors $\dim\left(\bigoplus_{i=1}^{k} E_i\right) = \sum_{i=1}^{k} \dim(E_i)$;
- réciproquement si $\dim(E_1 + \cdots + E_k) = \sum_{i=1}^{k} \dim(E_i)$ alors la somme est directe

Définition 9 — *Projections*

Si $E = \bigoplus_{k=1}^{n} E_k$, et $x \in E$, il existe une unique décomposition $x = x_1 + \cdots + x_n$ avec $x_i \in E_i$ pour tout $i \in [\![1, n]\!]$. L'application $x \mapsto x_i$ est **la projection sur E_i dans la décomposition** $E = \bigoplus_{k=1}^{n} E_k$.

Voici une nouvelle façon de définir une application linéaire...

Proposition 6 — Application linéaire définie par ses restrictions

Si $E = \bigoplus_{k=1}^{n} E_k$ et pour tout $i \in [\![1, n]\!]$, $v_i \in \mathcal{L}(E_i, F)$, alors il existe une unique application linéaire de E dans F dont la restriction à chaque E_i vaut v_i.

Preuve : Analyse-synthèse... ■

Par exemple, si $E = E_1 \oplus E_2$, il existe une unique application égale à l'identité sur E_1 et $-\mathrm{Id}$ sur E_2 (vous la reconnaissez ?). Dans le chapitre sur la réduction, le but du jeu sera, à u donnée, de découper l'espace sous la forme $E = \bigoplus_{k=1}^{n} E_k$, avec pour tout i la restriction de u à E_i le plus simple possible (idéalement : $\lambda_i \mathrm{Id}_{E_i}$).

1.7 Le théorème du rang revisité

Rappel : Le **rang d'une famille de vecteurs** est la dimension de l'espace qu'elle engendre. Le **rang d'une application linéaire** est la dimension de son image (lorsqu'elle est finie). C'est aussi le rang de l'image d'une base ou plus simplement d'une famille génératrice...
Les résultats suivants ne doivent pas nécessairement être connus, mais leurs preuves doivent être maîtrisées.

Exercice 14. *Soient $u \in \mathcal{L}(E,F)$ et $v \in \mathcal{L}(F,G)$. Montrer que :*
- *si u est surjective (a fortiori si c'est un isomorphisme), alors* $\mathrm{rg}(v \circ u) = \mathrm{rg}(v)$;
- *si v est injective (a fortiori si c'est un isomorphisme), alors* $\mathrm{rg}(v \circ u) = \mathrm{rg}(u)$.

Solution : Dans le premier cas, $\mathrm{rg}(v \circ u) = \dim(v(u(E))) = \dim(v(F)) = \mathrm{rg}(v)$ et dans le second cas, l'injectivité de v assure que $v(F_1)$ a la même dimension que F_1 pour tout sous-espace F_1 de F, et en particulier pour $F_1 = \mathrm{Im}\, u$. *(On avait bien entendu préalablement dessiné trois patates.)*

Exercice 15. *Soient $u \in \mathcal{L}(E,F)$ et $e_1, ..., e_k \in E$.*
1. *Montrer que le rang de $(u(e_1), ..., u(e_k))$ est majoré par celui de $(e_1, ..., e_k)$.*
2. *Montrer que si u est injective, alors il y a égalité.*

Solution : Extraire de $\mathcal{E} = (e_1, ..., e_k)$ une base $\mathcal{E}'$ de $\mathrm{Vect}(\mathcal{E})$: $u(\mathcal{E}')$ est alors une famille génératrice de $\mathrm{Vect}(u(\mathcal{E}))$...

Théorème 7 — *Théorème (formule) du rang*

Si $u \in \mathcal{L}(E,F)$ avec E de dimension finie, alors $\mathrm{Im}(u)$ est de dimension finie, et

$$\mathrm{rg}(u) = \dim(E) - \dim(\mathrm{Ker}(u)).$$

Bref : les degrés de liberté au départ qu'on ne retrouve pas dans l'image ne sont pas vraiment perdus : on les retrouve dans le noyau.

Preuve : Utiliser « la version géométrique du théorème du rang » qui va suivre ! (Terme usuel plus que contestable, dans la mesure où il ne fait pas intervenir le rang... mais disons qu'en dimension finie, il dit la même chose... en mieux !) ■

Remarque : Ainsi, comme on l'a vu plus tôt, si $u \in \mathcal{L}(E,F)$ avec E et F de dimensions finies **et égales**, il y a équivalence entre injectivité, surjectivité et bijectivité. C'est en particulier le cas pour les endomorphismes en dimension finie. Attention, $P \in \mathbb{K}[X] \mapsto P'$ est surjectif sans être injectif (endomorphisme... en dimension infinie).
Il est parfois intéressant d'appliquer le théorème du rang à des restrictions...

Exercice 16. *Soit $u \in \mathcal{L}(E)$, avec E un espace de dimension finie. Montrer :*

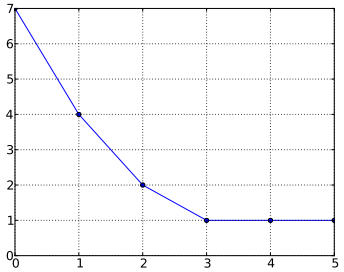
$$\forall n \in \mathbb{N}, \qquad \mathrm{rg}(u^{n+1}) - \mathrm{rg}(u^{n+2}) \leqslant \mathrm{rg}(u^n) - \mathrm{rg}(u^{n+1})$$

Solution : La formule du rang appliquée à la restriction de u à $\mathrm{Im}(u^n)$ donne :

$$\mathrm{rg}(u^n) - \mathrm{rg}(u^{n+1}) = \dim(\mathrm{Ker}(u) \cap \mathrm{Im}(u^n)).$$

On écrit la même chose au rang suivant, puis on utilise l'inclusion $\mathrm{Im}(u^{n+1}) \subset \mathrm{Im}(u^n)$.

Ainsi, la suite d'entiers $(\mathrm{rg}(u^n))_{n\in\mathbb{N}}$ est convexe : si on représente la ligne brisée correspondante, les segments on des pentes $\mathrm{rg}(u^{n+1}) - \mathrm{rg}(u^n)$ *négatives mais croissantes*, donc on obtiendra un aspect *convexe*, du type :



Exercice 17. *Comment réaliser ce graphique sous Python ?*

Une conséquence de ce résultat est d'ailleurs le fait vu plus haut : si $\mathrm{Im}(u^{n_0}) = \mathrm{Im}(u^{n_0+1})$, alors la suite des images itérées stagne à partir de ce rang.

Théorème 8 — *« La version géométrique du théorème du rang »*

Si $u \in \mathcal{L}(E,F)$ et que S est un supplémentaire de $\mathrm{Ker}\,(u)$, alors u induit un isomorphisme entre S et $\mathrm{Im}\,(u)$.

Preuve : Injectivité et surjectivité ! On notera que ce résultat est valable en dimension infinie pour E comme pour F, alors que dans la formule du rang on demande à E d'être de dimension finie (et pour cause !) ■

Rappelons qu'en dimension finie, on sait que $\mathrm{Ker}\,(u)$ possède un supplémentaire : on **commence** donc en général par fixer un tel supplémentaire avant d'aller plus loin (et pour la formule du rang, par exemple, on obtient $\mathrm{rg}(u) = \dim(S)$, et comme $E = \mathrm{Ker}\,(u) \oplus S$...).

1.8 Formes linéaires, hyperplans

Définition 10 — *Formes linéaires, hyperplans*

- Une **forme linéaire** sur E est une application linéaire de E dans $\mathbb{R}$. On note en général $E^* = \mathcal{L}(E,\mathbb{K})$ l'ensemble de ces formes linéaires.
- Un **hyperplan** est le noyau d'une forme linéaire non nulle.

Notons dès maintenant que l'image d'une forme linéaire non nulle est un sous-espace non nul de $\mathbb{K}$, donc c'est $\mathbb{K}$, qui est de dimension 1. Corollairement, la formule du rang nous assure que si E est de dimension finie n, alors ses hyperplans sont de dimension $n-1$. Réciproquement, si E est de dimension n et F en est un sous-espace de dimension $n-1$, alors c'est un hyperplan de E : on peut le voir de différentes façons ; par exemple en construisant une base de l'espace adaptée à F puis une forme linéaire dont le noyau sera F (ou comme conséquence du premier point de la proposition 7 à venir).

Exemples :

- Dans $\mathbb{K}^n$, les formes linéaires ont toutes la même tête : $(x_1,...,x_n) \mapsto \alpha_1 x_1 + \cdots \alpha_n x_n$.
- Dans $\mathbb{R}_n[X]$ les formes linéaires sont également toutes de la forme

$$p_0 + p_1 X + \cdots + p_n X^n \mapsto a_0 p_0 + \cdots + a_n p_n,$$

même si elles peuvent arriver masquées : $P \mapsto \displaystyle\int_0^1 P - P'(999)$ par exemple.

- Dans $\mathcal{M}_n(\mathbb{K})$, il y a la trace, ainsi que $M \mapsto \mathrm{tr}(AM)$ (à A fixé)... et on on peut montrer que c'est tout !
- D'une manière générale, en dimension finie il n'y a pas trop de suspens : E^* est de même dimension que E.
- Dans $\mathcal{C}([0,1],\mathbb{R})$ c'est nettement plus compliqué... En dimension infinie, on étudie souvent particulièrement les formes linéaires continues : attendre quelques mois ou années pour cela !

Proposition 7 — Supplémentaires d'hyperplans

Un sous-espace H de E est un hyperplan si et seulement s'il existe une droite vectorielle D telle que $H \oplus D = E$.

Preuve : Ce résultat peut sembler clair... mais seulement en dimension finie ! Sans cette hypothèse dimensionnelle, supposons d'abord $H = \mathrm{Ker}\,(\varphi)$, avec φ une forme linéaire non nulle. On choisit $x_0 \notin H$, et on montre par analyse-synthèse que H et $\mathbb{K}x_0$ sont supplémentaires. Dans l'autre sens, si $H \oplus \mathbb{K}x_0 = E$, tout élément x de E se décompose de façon unique sous la forme $x = h_1(x) + \varphi(x)x_0$, avec $h_1(x) \in H$ et $\varphi(x) \in \mathbb{K}$. On vérifie alors la linéarité de φ. Pour terminer, que vaut $\mathrm{Ker}\,(\varphi)$? ■

Remarque : Dans les espaces euclidiens (de dimension finie, muni d'un produit scalaire) on verra dans quelques mois que les formes linéaires sont toutes de la forme $\varphi_{u_0} : x \mapsto \langle u_0 | x \rangle$. L'application $\Phi : u_0 \mapsto \varphi_{u_0}$ fournit alors un isomorphisme naturel entre E et son dual.

Proposition 8 — Formes linéaires colinéaires

Deux formes linéaires non nulle φ_1 et φ_2 sont colinéaires si et seulement si elles ont le même noyau.

Preuve : Le sens direct est clair. Pour la réciproque, on peut par exemple prendre x_0 tel que $\mathbb{K}x_0$ soit un supplémentaire du noyau commun. Si on note K tel que $\varphi_2(x_0) = K\varphi_1(x_0)$, alors les formes linéaires $K\varphi_1$ et φ_2 coïncident sur deux sous-espaces supplémentaires... ■

2 Calcul matriciel

$$\begin{pmatrix} 3 & 4 \\ 6 & 8 \end{pmatrix}^2 = \begin{pmatrix} 33 & 44 \\ 66 & 88 \end{pmatrix}$$

2.1 Rappels de première année

Rappelons qu'une matrice $M \in \mathcal{M}_{n,p}$ peut permettre de représenter p vecteurs de E (de dimension n) dans une base de E, ou bien une application $u \in \mathcal{L}(E,F)$ (avec E et F de dimensions respectives p et n) entre des bases données de E et F : une telle matrice représente alors l'image par u de la base de E dans la base de F. Rappelons le résultat **le plus important** en calcul matriciel :

PROPOSITION 9 — Théorème fondamental du calcul matriciel

Pour écrire une matrice, DANS CET ORDRE :

1. On ouvre une grande parenthèse à gauche.
2. On la ferme un peu plus loin à droite.
3. On écrit des machins DESSUS la matrice (les vecteurs qu'on va représenter).
4. On écrit des machins À DROITE (la base dans laquelle les vecteurs vont être représentés).
5. On réalise alors que la taille de la matrice ne convient pas, et on ajuste.
6. On fait des petits calculs.
7. On écrit des machins DANS la matrice.

PREUVE : Sinon, ça ne marche pas (vous l'avez normalement déjà constaté). ■

EXEMPLES :

— Si on munit $E = \mathbb{R}^3$ et $F = \mathbb{R}^2$ de leurs bases canoniques respectives $\mathcal{E}$ et $\mathcal{F}$, les matrices $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ représentent respectivement $u \in \mathcal{L}(E,F)$ (entre $\mathcal{E}$ et $\mathcal{F}$) et $v \in \mathcal{L}(F,E)$ (entre $\mathcal{F}$ et $\mathcal{E}$), avec :

$$u \left\| \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^2 \\ (x_1,x_2,x_3) & \longmapsto & (x_1+2x_2+3x_3, 4x_1+5x_2+6x_3) \end{array} \right.$$

et

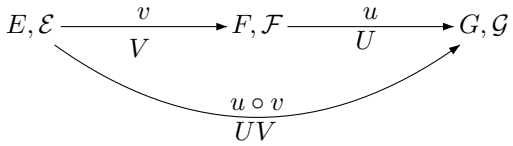
$$v \left\| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ (x_1,x_2) & \longmapsto & (x_1+2x_2, 3x_1+4x_2, 5x_1+6x_2) \end{array} \right. .$$

Fondamentalement, u est l'application $X \mapsto AX$, de $\mathcal{M}_{3,1}(\mathbb{R})$ dans $\mathcal{M}_{2,1}(\mathbb{R})$, si on confond un habitant de $\mathbb{K}^n$ avec une matrice colonne de $M\mathcal{M}_{n,1}(\mathbb{K})$ (ce qui est souvent raisonnable !)

— La matrice colonne $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ représente $(1,2,3)$ dans la base canonique de $\mathbb{R}^3$, mais également $1 + 2X + 3X^2$ dans la base $(1, X, X^2)$ de $\mathbb{R}_2[X]$, ainsi que $3 + 2X + X^2$ dans la base $(X^2, X, 1)$ de $\mathbb{R}_2[X]$...

— La matrice $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ représente la forme linéaire $(x_1,x_2,x_3) \mapsto x_1 + 2x_2 + 3x_3$ entre la base canonique de $\mathbb{R}^3$ et $\mathbb{R}$ muni de la base que je vous laisse deviner...

La somme et la multiplication de deux matrices sont alors définies pour faire en sorte que la matrice d'une somme (respectivement d'une composée) soit la somme (respectivement le produit) des matrices. Sur la question du produit, il faut retenir un peu mieux que « ça se passe bien » ou encore : « $\mathrm{Mat}(u \circ v) = \mathrm{Mat}(u)\,\mathrm{Mat}(v)$ ». Ce qu'il faut retenir, c'est :
Ça se passe bien, comme indiqué sur le schéma suivant :



C'est-à-dire plus précisément (lire le dessin !) : « Si $v \in \mathcal{L}(E,F)$, $u \in \mathcal{L}(F,G)$, avec $\mathcal{E}$, $\mathcal{F}$ et $\mathcal{G}$ des bases de E, F et G, alors : $\mathrm{Mat}(u \circ v, \mathcal{E}, \mathcal{G}) = \mathrm{Mat}(u, \mathcal{F}, \mathcal{G})\,\mathrm{Mat}(v, \mathcal{E}, \mathcal{F})$ »
De même si x a pour coordonnées $X \in \mathcal{M}_{p,1}(\mathbb{K})$ dans une base $\mathcal{E}$ de E et $u \in \mathcal{L}(E,F)$, alors les coordonnées de $u(x)$ dans une base $\mathcal{F}$ de F sont (comme on peut l'espérer) dans la matrice UX, avec $U = \mathrm{Mat}(u, \mathcal{E}, \mathcal{F})$.
L'ensemble $E = \mathcal{M}_n(\mathbb{K})$ des matrices carrées (n,n) constitue une algèbre (espace vectoriel + anneau) de neutre I_n. La **trace** d'une matrice carrée est... ce que l'on sait (ou pas) : la somme de ses éléments diagonaux.
Les matrices possédant un symétrique pour la loi « . » sont dites inversibles.

Exercice 18. *On suppose que $A, B \in \mathcal{M}_n(\mathbb{K})$ vérifient $AB = I_n$. Montrer : $BA = I_n$.*

On va fréquemment changer de base : on veut un résultat dans une base, mais on préfère travailler dans une autre, plus adaptée à la géométrie du problème, avant de revenir à la base de départ.

Définition 11 — *Matrices de passage*

Si $\mathcal{E}$ et $\mathcal{F}$ sont deux bases d'un même espace E, la **matrice de passage** de $\mathcal{E}$ vers $\mathcal{F}$ est la matrice représentant $\mathcal{F}$ (« nouvelle base ») dans $\mathcal{E}$ (« ancienne base »).

Si $\mathcal{E}$ et $\mathcal{F}$ sont deux bases d'un même espace E, on peut s'intéresser à la matrice représentant l'identité entre $\mathcal{E}$ et $\mathcal{F}$: elle représente la base $\mathcal{E}$ dans la base $\mathcal{F}$, donc c'est la matrice de passage de $\mathcal{F}$ vers $\mathcal{E}$, **et non l'inverse**. On retiendra donc :

$$\underset{\mathcal{E}\to\mathcal{F}}{\mathrm{Pas}} = \mathrm{Mat}(\mathrm{Id}, \mathcal{F}, \mathcal{E}), \qquad \underset{\mathcal{F}\to\mathcal{E}}{\mathrm{Pas}} = \mathrm{Mat}(\mathrm{Id}, \mathcal{E}, \mathcal{F}).$$

Fait : Si on connaît *presque* la définition d'une matrice de passage, ou qu'on a *pas trop* envie de réfléchir, alors on est *à peu près* certain de se tromper dans la formule précédente... et surtout la suivante.

Théorème 9 — *Changement de base*

Soient E et F deux espaces vectoriels. E est muni de deux bases $\mathcal{B}_1$ et $\mathcal{B}'_1$, alors que F est muni des bases $\mathcal{B}_2$ et $\mathcal{B}'_2$. On note P (resp. Q) la matrice de passage entre $\mathcal{B}_1$ et $\mathcal{B}'_1$ (resp. $\mathcal{B}_2$ et $\mathcal{B}'_2$). Soit $u \in \mathcal{L}(E,F)$. On suppose que $M = \mathrm{Mat}(u, \mathcal{B}_1, \mathcal{B}_2)$ et $M' = \mathrm{Mat}(u, \mathcal{B}'_1, \mathcal{B}'_2)$. Alors :

$$QM' = MP.$$

$$\begin{array}{ccc} E, \mathcal{B}_1 & \xrightarrow[M]{u} & F, \mathcal{B}_2 \\ {\scriptstyle \mathrm{Id}_E}\uparrow P & & {\scriptstyle \mathrm{Id}_F}\uparrow Q \\ E, \mathcal{B}'_1 & \xrightarrow[M']{u} & F, \mathcal{B}'_2 \end{array}$$

Preuve : On a $\mathrm{Id}_F \circ u = u \circ \mathrm{Id}_E$: il reste à appliquer la formule donnant la matrice d'une composée... mais pour cela, il faut savoir ce qu'est une matrice de passage. Et pas *approximativement...* ■

La proposition suivante est une simple conséquence du résultat précédent, mais est importante : la plupart du temps on change de bases pour des endomorphismes.

Proposition 10 — Changement de base – cas des endomorphismes

Soit $u \in \mathcal{L}(E)$, avec E un espace vectoriel muni de deux bases $\mathcal{E}$ et $\mathcal{E}'$. On note P la matrice de passage de $\mathcal{E}$ vers $\mathcal{E}'$. Si on définit de plus $M = \mathrm{Mat}(u, \mathcal{E})$ et $M' = \mathrm{Mat}(u, \mathcal{E}')$, alors :

$$M' = P^{-1}MP.$$

Proposition 11 — Plusieurs matrices ; une seule trace

Si $u \in \mathcal{L}(E)$, les matrices représentant u dans toutes les bases de E ont la même trace.

Preuve : Si $\mathcal{E}$ et $\mathcal{E}'$ sont deux bases de E, $P = \underset{\mathcal{E}\to\mathcal{E}'}{\mathrm{Pas}}$, $M = \mathrm{Mat}(u, \mathcal{E})$ et $M' = \mathrm{Mat}(u, \mathcal{E}')$, alors $M' = P^{-1}MP$. On prouve par ailleurs que $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, donc :

$$\mathrm{tr}(M') = \mathrm{tr}(P^{-1}MP) = \mathrm{tr}\left((P^{-1}M)P\right) = \mathrm{tr}\left(P(P^{-1}M)\right) = \mathrm{tr}(M).$$

■

Définition 12 — *Trace d'un endomorphisme*

La **trace d'un endomorphisme** est la trace (commune) des matrices qui le représentent.

Exemples :
- Si p est une projection, alors sa trace est égale à son rang.
- Si s est une symétrie par rapport à un sous-espace de dimension p, et que n est la dimension de l'espace ambiant, alors $\mathrm{tr}(s) = 2p - n$ (mais n'allez pas retenir ce résultat absurde).
- La trace de l'endomorphisme de $\mathbb{K}_n[X]$ $P \mapsto P'$ est nulle.

Exercice 19. *Déterminer la trace de l'application $M \in \mathcal{M}_n(\mathbb{K}) \mapsto \mathrm{tr}(M)I_n$.*

2.2 Opérations élémentaires

Les opérations que l'on fait sur les lignes et colonnes des matrices sont essentiellement celles qu'on fait dans la manipulation des systèmes linéaires, quand on pivote (on donne ici celles sur les colonnes, mais il y a bien entendu les mêmes sur les lignes) :
- des **transvections** $C_i \leftarrow C_i + \lambda C_j$ $(i \neq j)$;
- des **dilatations** $C_i \leftarrow \lambda C_i$ $(\lambda \neq 0)$;
- des **échanges** $C_i \leftrightarrow C_j$ $(i \neq j)$.

Il s'agit clairement d'opérations **réversibles** (on peut revenir à la matrice initiale par des opérations de même nature.

Exercice 20. *Soit $M \in \mathcal{M}_n(\mathbb{K})$. Calculer AM et MA lorsque $A = T_{i,j,\lambda} := I_n + \lambda E_{i,j}$, puis $A = D_{i,\lambda} := I_n + (1-\lambda)E_{i,i}$ et $A = S_{i,j} := I_n + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}$.*

Exercice 21. *Vérifier que les matrices $T_{i,j,\lambda}$, $D_{i,\lambda}$ et $S_{i,j}$ sont inversibles (avec $i \neq j$ et $\lambda \neq 0$).*

Ainsi [7], les opérations élémentaires correspondent à des multiplications (à droite ou à gauche) par des matrices inversibles ; on retrouve ainsi le caractère *réversible* des dites opérations [8].

2.3 Autour du rang

Définition 13 — *Rang d'une matrice*

Le rang d'une matrice de $\mathcal{M}_{n,p}(\mathbb{K})$ est le rang de l'application linéaire canoniquement associée (appartenant donc à $\mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$).

7. Les vérifications n'ont été faites que dans le cas de matrices carrées, mais c'est la même chose dans $\mathcal{M}_{n,p}(\mathbb{K})$ lorsque $n \neq p$.

8. On peut même obtenir le caractère inversible des matrices en pensant justement aux opérations inverses, qui fournissent de bonnes candidates comme matrices inverses.

C'est bien entendu également le rang de la famille des « vecteurs-colonne » de la matrice, c'est-à-dire des p vecteurs de $\mathbb{R}^n$ représentés par la matrice en question dans la base canonique de $\mathbb{R}^n$.

Il serait souhaitable de pouvoir relier le rang des matrices d'une part, et celui des applications linéaires et familles de vecteurs d'autre part... au delà de l'espace $\mathbb{K}^n$ muni de sa base canonique. Le résultat suivant dit que tout se passe comme on peut raisonnablement l'espérer...

THÉORÈME 10 — *Les rangs sont bien ce qu'on espère*

> Le rang d'une application linéaire est le rang de toute matrice la représentant entre deux bases. Celui d'une famille de vecteurs est celui de la matrice la représentant dans n'importe quelle base.

PREUVE : Supposons que $u \in \mathcal{L}(E,F)$ a pour matrice U entre deux bases $\mathcal{E}$ et $\mathcal{F}$, notons $\mathcal{B}$ et $\mathcal{B}'$ les bases canoniques de $\mathbb{K}^p$ et $\mathbb{K}^n$, et v l'application linéaire canoniquement associée à U. Regardons maintenant droit dans les yeux le diagramme suivant :

$$\begin{array}{ccc} E,\mathcal{E} & \xrightarrow[U]{u} & F,\mathcal{F} \\ {\scriptstyle\Phi}\uparrow & & {\scriptstyle\Psi}\uparrow \\ \mathbb{K}^p,\mathcal{B} & \xrightarrow[U]{v} & \mathbb{K}^n,\mathcal{B}' \end{array}$$

Il y a une application Φ naturelle (dans ce contexte) entre $\mathbb{K}^p$ et E ; même chose entre $\mathbb{K}^n$ et F. Les matrices de Φ et Ψ sont assez simples. Compléter alors le diagramme, regarder $u \circ \Phi$ et $\Psi \circ v$, plisser les yeux, puis conclure en hochant la tête avec un air intelligent. ■

REMARQUES :

- Le rang d'une matrice de la forme $\begin{pmatrix} T & \vdots & M \\ \cdots & \cdots & \cdots \\ 0_{n-r,r} & \vdots & 0_{n-r,p-r} \end{pmatrix}$, avec $T \in \mathcal{M}_r(\mathbb{K})$ triangulaire à coefficients diagonaux non nuls... vaut r (pourquoi, au fait ?).
- Le rang est invariant par opérations élémentaires (pourquoi ?).
- En combinant les deux remarques précédentes et un procédé parfois utilisé en algèbre linéaire (...), on obtient un algorithme pour calculer le rang d'une matrice.

EXEMPLE :

$$M = \begin{pmatrix} 1 & 1 & 5 \\ -1 & 2 & 1 \\ 1 & 5 & 13 \end{pmatrix} \xrightarrow[L_3 \leftarrow L_3 - L_1]{L_2 \leftarrow L_2 + L_1} \begin{pmatrix} 1 & 1 & 5 \\ 0 & 3 & 6 \\ 0 & 4 & 8 \end{pmatrix} \xrightarrow{L_3 \leftarrow 3L_3 - 4L_2} \begin{pmatrix} 1 & 1 & 5 \\ 0 & 3 & 6 \\ 0 & 0 & 0 \end{pmatrix},$$

et donc : $\mathrm{rg}(M) = 2$.

THÉORÈME 11 — *Réduction du rang*

> Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang r, alors il existe $P \in \mathrm{GL}_n(\mathbb{K})$ et $Q \in \mathrm{GL}_p(\mathbb{K})$ tels que
>
> $$PAQ = J_r := \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix} \in \mathcal{M}_{n,p}(\mathbb{K})$$

PREUVE :

- Géométriquement : on considère l'application linéaire canoniquement associée à A, et on construit des bases adaptées, de $\mathbb{K}^p$ et $\mathbb{K}^n$, entre lesquelles la matrice de l'application est J_r (micro analyse-synthèse). Il reste à appliquer la formule de changement de base.
- Algorithmiquement : on pivote pour transformer A en J_r (la première phase est la même que pour le calcul du rang, puis on dilate et opère sur les colonnes). Chaque opération est une multiplication à gauche ou à droite par une matrice inversible. On a donc finalement après s opérations sur les lignes et t sur les colonnes : $P_s...P_2P_1.A.Q_1...Q_t = J_r$, et c'est gagné.

■

EXEMPLE : Traitons de deux façons $A = \begin{pmatrix} 1 & 3 \\ 2 & 2 \\ 1 & 1 \end{pmatrix}$:

— Par pivot :

$$\begin{pmatrix}1&3\\2&2\\1&1\end{pmatrix} \xrightarrow[L_3\leftarrow L_3-L_1]{L_2\leftarrow L_2-2L_1} \begin{pmatrix}1&3\\0&-4\\0&-2\end{pmatrix} \xrightarrow[L_2\leftarrow(-1/4)L_2]{L_3\leftarrow 2L_3-L_2} \begin{pmatrix}1&3\\0&1\\0&0\end{pmatrix} \xrightarrow{C_2\leftarrow C_2-3C_1} \begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix}$$

On obtient la matrice $P = P_4...P_1I_3$ on réalisant les opérations sur les lignes sur la matrice I_3 :

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \xrightarrow[L_3\leftarrow L_3-L_1]{L_2\leftarrow L_2-2L_1} \begin{pmatrix}1&0&0\\-2&1&0\\-1&0&1\end{pmatrix} \xrightarrow[L_2\leftarrow(-1/4)L_2]{L_3\leftarrow 2L_3-L_2} \begin{pmatrix}1&0&0\\1/2&-1/4&0\\0&-1&2\end{pmatrix} = P$$

et de même, $Q = I_2Q_1$ s'obtient en réalisant l'unique opération sur la colonne sur la matrice I_2 :

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} \xrightarrow{C_2\leftarrow C_2-3C_1} \begin{pmatrix}1&-3\\0&1\end{pmatrix} = Q$$

Vérification avec Python (les matrices disposent d'une méthode pour être multipliées) :

```
from numpy import array

P = array( [[1, 0, 0], [0.5, -0.25, 0], [0, -1, 2]])
A = array([[1, 3], [2, 2], [1, 1]])
Q = array([[1, -3], [0, 1]])

"""
>>> P.dot(A).dot(Q)
array([[ 1.,  0.],
       [ 0.,  1.],
       [ 0.,  0.]])
"""
```

— Soient u l'application linéaire canoniquement associée à A, $\mathcal{E} = (e_1, e_2)$ la base canonique de $E = \mathbb{R}^2$ et $\mathcal{F} = (f_1, f_2, f_3)$ la base canonique de $F = \mathbb{R}^3$. La matrice A est clairement de rang 2 : son noyau est réduit à $\{0\}$. On prend donc comme nouvelle base au départ $\mathcal{E}_1 = \mathcal{E}$, et comme nouvelle base à l'arrivée : $\mathcal{F}_1 = (u(e_1), u(e_2), f_3)$. On a alors $\mathrm{Mat}(u, \mathcal{E}_1, \mathcal{F}_1) = \begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix} = J_2$.
Notre diagramme préféré nous dit qu'en notant $Q_1 = \underset{\mathcal{E}\to\mathcal{E}_1}{\mathrm{Pas}} = I_2$ et $P_1 = \underset{\mathcal{F}\to\mathcal{F}_1}{\mathrm{Pas}} = \begin{pmatrix}1&3&0\\2&2&0\\1&1&1\end{pmatrix}$ on aura $AQ_1 = P_1J_2$.

$$\begin{array}{ccc} E,\mathcal{E} & \xrightarrow[A]{u} & F,\mathcal{F} \\ {\scriptstyle \mathrm{Id}_E}\uparrow{\scriptstyle Q_1} & & {\scriptstyle \mathrm{Id}_F}\uparrow{\scriptstyle P_1} \\ E,\mathcal{E}_1 & \xrightarrow[J_2]{u} & F,\mathcal{F}_1 \end{array}$$

Pour avoir $PAQ = J_2$, il **suffit** donc de prendre $P = P_1^{-1}$ et $Q = Q_1 = I_2$.

```
P1 = array([[1, 3, 0], [2, 2, 0], [1, 1, 1]])

"""
>>> inv(P1).dot(A)
array([[ 1.,  0.],
       [ 0.,  1.],
       [ 0.,  0.]])
"""
```

Exercice 22. *Montrer que le rang de toute matrice est égal au rang de sa transposée.*

2.4 Matrices et endomorphismes de rang 1

Il n'y a rien spécifiquement au programme sur cette question, mais les résultats qui vont constituer les exos suivants sont très classiques et souvent utiles. Une bonne compréhension de la géométrie de ces endomorphismes peut être souvent salvatrice.
On commence par un résultat purement matriciel

PROPOSITION 12 — Une caractérisation des matrices de rang 1

Une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang 1 si et seulement si elle s'écrit CL, avec $C \in \mathcal{M}_{n,1}(\mathbb{K})$ et $L \in \mathcal{M}_{1,p}(\mathbb{K})$ non nulles.

PREUVE : Tout d'abord, si $A = CL$ avec C et L comme dans l'énoncé, alors toutes les colonnes de A sont colinéaires à C (et il en existe au moins une non nulle) donc A est de rang 1. Réciproquement, supposons A de rang 1. Au choix :

- On le prouve dans le cas particulier $J_1 = C_1 L_1$, et on traite le cas général via $A = PJ_1Q = (PC_1)(L_1Q)$.
- Toutes les colonnes de A sont colinéaires, donc de la forme $\lambda_i C$ pour une certaine $C \in \mathcal{M}_{n,1}(\mathbb{K})$. Il reste à prendre $L = \begin{pmatrix}\lambda_1 & \dots & \lambda_p\end{pmatrix}$

■

EXEMPLE :

$$\begin{pmatrix}-2 & -1 & 1 & -3\\ 4 & 2 & -2 & 6\\ -6 & -3 & 3 & -9\end{pmatrix} = \begin{pmatrix}1\\ -2\\ 3\end{pmatrix} \begin{pmatrix}-2 & -1 & 1 & -3\end{pmatrix}$$

Le résultat suivant est souvent demandé, que ce soit pour des matrices ou des endomorphismes.

Exercice 23. *Soit A une matrice de rang 1. Montrer :*

$$A^2 = (\mathrm{tr}A)A$$

On pourra utiliser la décomposition $A = CL$, ou travailler dans une base adaptée à l'endomorphisme canoniquement associé à A, qui part d'une base du noyau... ou de l'image, d'ailleurs !

Terminons par ce résultat, qui dit qu'il y a essentiellement deux types très différents d'endomorphismes de rang 1, selon que l'image est ou non incluse dans le noyau.

Exercice 24. *Soit A une matrice de rang 1. Montrer que A est semblable à*

$$\begin{pmatrix}\mathrm{tr}(A) & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0\end{pmatrix} \quad \textit{ou} \quad \begin{pmatrix}0 & \cdots & 0 & 1\\ & (0) & & 0\\ & & (0) & \vdots\\ 0 & \cdots & 0 & 0\end{pmatrix}$$

Dans chaque cas, dessiner l'image et le noyau de l'endomorphisme canoniquement associé à A.

Terminons par une description géométrique raisonnable des endomorphismes de rang 1 (on aurait pu commencer par ça).

Exercice 25. *Soit $u \in \mathcal{L}(E)$ de rang 1. Montrer qu'il existe une forme linéaire $\varphi \in \mathcal{L}(E, \mathbb{K})$non nulle et $f_0 \in E$ non nul tels que :*

$$\forall x \in E, \qquad u(x) = \varphi(x) f_0$$

2.5 Diverses choses

Comme $\mathcal{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre, on peut parler de « polynômes évalués en une matrice ». De telles matrices interviennent dans de nombreuses situations. Si $P \in \mathbb{K}[X]$ et $A \in \mathcal{M}_n(\mathbb{K})$, $P(A)$ est « ce qu'on imagine », mais définissez-le tout de même formellement !
EXEMPLES :

- Le calcul de A^n peut se faire en calculant le reste dans la division euclidienne de X^n par un polynôme annulateur de A : il suffit d'évaluer ce reste en A.

— Si $A \in \mathcal{M}_n(\mathbb{K})$, on est certain que toutes les matrices de la forme $P(A)$, avec $P \in \mathbb{K}[X]$, commutent avec A. On verra que dans certaines circonstances se sont les seules (mais ce n'est pas toujours le cas : prendre $A = I_n$ par exemple !).

Ce qu'on utilise en permanence – en général sans s'en rendre compte – c'est que $(\lambda P + Q)(A) = \lambda P(A) + Q(A)$ et $(PQ)(A) = P(A)Q(A)$ pour tous gnagna. De façon snob, on dit que $P \mapsto P(A)$ est un morphisme d'algèbre.

Exercice 26. *CCINP 2007 : Soit* $A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}$. *Calculer* A^n *pour* $n \in \mathbb{N}$.

En général, deux matrices n'ont aucune raison de commuter. Les matrices de la forme λI_n commutent tout de même avec toutes les autres ; par ailleurs, une matrice donnée A commute certes avec elle-même, mais aussi avec son carré, son cube... et n'importe quel « polynôme en A ».

Exercice 27. *Déterminer l'ensemble des matrices commutant avec la matrice diagonale* $Diag(1, 2, ..., n)$.

Est-ce qu'il existe des matrices autres que λI_n qui commutent avec toutes les autres ?

Exercice 28. *Soit* $A \in \mathcal{M}_n(\mathbb{K})$ *commutant avec toutes les autres matrices de* $\mathcal{M}_n(\mathbb{K})$. *En calculant* $AE_{i,j}$ *et* $E_{i,j}A$, *montrer que* A *est diagonale, puis scalaire (i.e. : de la forme* λI_n*).*

Le résultat suivant est un **très** grand classique

Exercice 29. *Critère d'Hadamard (ou de la diagonale dominante)*
Soit $A \in \mathcal{M}_n(\mathbb{C})$ *telle que :*

$$\forall i \in [\![1, n]\!], \qquad |a_{i,i}| > \sum_{j \neq i} |a_{i,j}| .$$

Montrer que A *est inversible.*

Solution : Soit u canoniquement associée à A. On va montrer que u est injective. Pour cela, on prend un habitant du noyau. La relation $u(x) = 0$ (ou encore $AX = 0$, avec $X \in \mathcal{M}_{n,1}(\mathbb{K})$ constitué des coordonnées de x dans la base canonique de $\mathbb{C}^n$) fournit n relations. C'est l'élément central $a_{i,i}x_i$ de la relation qui est censé être gros... si x_i n'est pas trop petit. On choisit donc i_0 tel que $|x_{i_0}|$ soit maximal : en isolant le terme $a_{i_0,i_0}x_{i_0} = -\sum_{j \neq i_0} a_{i_0,j}x_j$ et en inégalitétriangularisant à droite, on obtient une contradiction si $x_{i_0} \neq 0$.

2.6 Déterminants

2.6.1 Micro-théorie

Définition 14 — *Formes multilinéaires*

Soit E un espace vectoriel de dimension n. Une **forme multilinéaire** sur E est une application de E^n dans E linéaire par rapport à chacune de ses variables. Elle est dite **alternée** lorsque $f(v_1, ..., v_n) = 0$ dès qu'il existe $i \neq j$ tel que $v_i = v_j$. Elle est dite **antisymétrique** lorsque pour tout $i < j$, $f(v_1, ..., v_i, ..., v_j, ..., v_n) = -f(v_1, ..., v_j, ..., v_i, ..., v_n)$.

Notons que pour les corps honnêtes (ceux dans lesquels on peut diviser par deux sans se faire gronder, en particulier $\mathbb{R}$ et $\mathbb{C}$), il y a équivalence entre le fait d'être alterné et celui d'être antisymétrique (le vérifier !). Pour $E = \mathbb{R}^2$, l'application $f : ((a, b), (c, d)) \mapsto ad - bc$ est bilinéaire alternée.
Remarque : Arrivé ici, la simple existence d'une forme bilinéaire alternée non nulle ne va pas de soi !

Théorème 12 — *Vers le déterminant*

Si $\mathcal{E}$ est une base de E, alors il existe une unique forme multilinéaire alternée f telle que $f(\mathcal{E}) = 1$.

Preuve : Ce résultat est admis : il peut se prouver par analyse (qui donne l'unicité et le seul candidat acceptable) puis synthèse (où on constate que le candidat précédent répond au cahier des charges). En fait, sans la condition portant sur $f(\mathcal{E})$, l'ensemble des formes multilinéaires alternées est une droite vectorielle. ■

Définition 15 — *Déterminants de n vecteurs dans une base*

Si $\mathcal{E}$ est une base de E, l'application $\det_{\mathcal{E}}$ est l'unique forme multilinéaire alternée telle que $\det_{\mathcal{E}}(\mathcal{E}) = 1$.

Que se passe-t-il si $\mathcal{E}'$ est une autre base ? On a $\det_{\mathcal{E}'} = K \det_{\mathcal{E}}$, donc en évaluant en $\mathcal{E}$: $\det_{\mathcal{E}'}(\mathcal{E}) = K$. Il vient alors $\det_{\mathcal{E}} = \det_{\mathcal{E}'}(\mathcal{E}) \det_{\mathcal{E}}$, puis en évaluant en $\mathcal{E}'$: $1 = \det_{\mathcal{E}'}(\mathcal{E}) \det_{\mathcal{E}}(\mathcal{E}')$. On en déduit entre autre que $\det_{\mathcal{E}}(\mathcal{E}') \neq 0$: le déterminant (dans une base) d'une famille qui est une base... est non nul.

Théorème 13 — *Être ou ne pas être (une base)*

Une famille $\mathcal{F}$ est une base si et seulement si son déterminant dans une base est non nul.

Preuve : En fait, dès que le déterminant dans UNE base est non nul, son déterminant dans TOUTE base est non nul. On a déjà vu le sens « si je suis une base, alors mon déterminant est non nul ». On prouve la réciproque par l'absurde : si une famille $\mathcal{F}$ n'est pas une base, alors elle est liée (elle possède n vecteurs, tout de même !), donc par exemple f_1 est combinaison linéaire de $f_2, ..., f_n$. On a alors :

$$\det_{\mathcal{E}}(\mathcal{F}) = \det_{\mathcal{E}}(\lambda_1 f_2 + \cdots + \lambda_n f_n, f_2, ..., f_n) = \lambda_1 \det_{\mathcal{E}}(f_2, f_2, ..., f_n) + \cdots + \lambda_n \det_{\mathcal{E}}(f_n, f_2, ..., f_n) = 0$$

du fait du caractère alterné. ■

Si $u \in \mathcal{L}(E)$ et $\mathcal{E}$ est une base, alors l'application $\varphi_{\mathcal{E}} : (v_1, ..., v_n) \mapsto \det_{\mathcal{E}}(u(v_1), ..., u(v_n))$ est multilinéaire alternée, donc de la forme $K_{\mathcal{E}} \det_{\mathcal{E}}$. Ce qui est remarquable, c'est que $K_{\mathcal{E}}$ ne dépend pas de $\mathcal{E}$: si $\mathcal{E}$ et $\mathcal{F}$ sont deux bases, alors :

$$\begin{aligned} K_{\mathcal{E}} &= \det_{\mathcal{E}}(u(e_1), ..., u(e_n)) = \det_{\mathcal{E}}(\mathcal{F}) \det_{\mathcal{F}}(u(e_1), ..., u(e_n)) \\ &= \det_{\mathcal{E}}(\mathcal{F}) K_{\mathcal{F}} \det_{\mathcal{F}}(e_1, ..., e_n) = \det_{\mathcal{E}}(\mathcal{F}) K_{\mathcal{F}} \det_{\mathcal{F}}(\mathcal{E}) = K_{\mathcal{F}}. \end{aligned}$$

Définition 16 — *Déterminant d'un endomorphisme*

Si $u \in \mathcal{L}(E)$, le **déterminant** de u est le scalaire K tel que pour toute base $\mathcal{E}$ de E et tout $(v_1, ..., v_n) \in E^n$, $\det_{\mathcal{E}}(u(v_1), ..., u(v_n)) = K \det_{\mathcal{E}}(v_1, ..., v_n)$.

Le déterminant peut donc être vu comme un facteur de dilatation de volumes (si on est en base orthonormée dans un euclidien, $|\det_{\mathcal{E}}(v_1, ..., v_n)|$ est le volume du parallélépipède de base les v_i).
Les résultats qui suivent sont des conséquences assez simples de ce qui précède :

Proposition 13 — Déterminant d'une composée

- Si $u, v \in \mathcal{L}(E)$, alors $\det(u \circ v) = \det(u) \det(v)$.
- Un endomorphisme u est bijectif si et seulement si son déterminant est non nul.

Tout cela est bien gentil... mais comment calculer les déterminants ?

Définition 17 — *Déterminant d'une matrice*

Le **déterminant d'une matrice carrée** est le déterminant de l'application linéaire canoniquement associée (qui est bien un endomorphisme).

On a alors plus ou moins directement :

Proposition 14 — Propriétés bien connues du déterminant

- Si $A, B \in \mathcal{M}_n(\mathbb{K})$, alors $\det(AB) = \det(A) \det(B)$.
- Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si son déterminant est non nul.
- Les transvections $C_i \leftarrow C_i + \lambda C_j$ conservent le déterminant. Les échanges $C_i \leftrightarrow C_j$ changent les déterminants en leur opposé ; les dilatations $C_i \leftarrow \lambda C_i$ multiplient les déterminants par λ.
- Le déterminant d'une matrice triangulaire est égal au produit des éléments diagonaux.
- Le déterminant d'une matrice est égal au déterminant de sa transposée.
- Les opérations sur les lignes ont les mêmes effets que les opérations sur les colonnes.

Remarques :
- On admettra que le déterminant d'un endomorphisme est celui de sa matrice dans n'importe quelle base ; ouf !
- Attention, $\det(\lambda A) = \lambda^n \det(A)$!
- De même, $\det(A+B)$ n'a aucune raison d'être égal à $\det(A) + \det(B)$!
- Pour ceux [9] qui ont des souvenirs des formules de Cramer : pour résoudre $AX = Y$, Cramer nous dit que lorsque $\det(A) \neq 0$, alors il existe une unique solution (ça, c'est clair !) avec $x_i = \dfrac{\det(A_i)}{\det(A)}$, où A_i est la matrice A dans laquelle on a remplacé la $i$ème colonne par Y. Pour comprendre cela, on peut réécrire $AX = Y$ sous la forme $x_1C_1 + \cdots + x_nC_n = Y$, avec $C_1, ..., C_n$ les colonnes de A. On a alors $\det(Y, C_2, ..., C_n) = x_1 \det(C_1, ..., C_n)$ par caractère multilinéaire alterné... ce qui est le résultat attendu !

2.6.2 In real life

En pratique, les calculs de déterminants se font :
- en pivotant pour faire apparaître des zéros : le plus possible sur une ligne ou une colonne, pas n'importe où/un peu partout (ça ne sert à rien) ;
- en développant selon les lignes/colonnes (par exemple une où on a placé beaucoup de zéros...) ;
- en factorisant sur des lignes ou colonnes :

$$\det(\lambda C_1 | C_2 | \cdots | C_n) = \lambda \det(C_1 | C_2 | \cdots | C_n)$$

Exemples :
- Vandermonde en dimension 3 : si $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$, alors :

$$\begin{aligned}\begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 \\ 1 & \lambda_2 & \lambda_2^2 \\ 1 & \lambda_3 & \lambda_3^2 \end{vmatrix} &= \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 \\ 0 & \lambda_2 - \lambda_1 & \lambda_2^2 - \lambda_1^2 \\ 0 & \lambda_3 - \lambda_1 & \lambda_3^2 - \lambda_1^2 \end{vmatrix} = (\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1) \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 \\ 0 & 1 & \lambda_2 + \lambda_1 \\ 0 & 1 & \lambda_3 + \lambda_1 \end{vmatrix} \\ &= (\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1) \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 \\ 0 & 1 & \lambda_2 + \lambda_1 \\ 0 & 0 & \lambda_3 - \lambda_2 \end{vmatrix} = (\lambda_2 - \lambda_1)(\lambda_3 - \lambda_1)(\lambda_3 - \lambda_2).\end{aligned}$$

- CCINP 2010 (PC) : Calculer le déterminant de M telle que $M_{i,j} = \begin{cases} \cos\alpha & \text{si } i = j = 1 \\ 2\cos\alpha & \text{si } i = j > 1 \\ 1 & \text{si } |i-j| = 1 \\ 0 & \text{sinon} \end{cases}$

  En développant selon la dernière colonne puis la dernière ligne, on trouve la relation de récurrence $D_n = 2\cos\alpha D_{n-1} - D_{n-2}$. On intuite alors le résultat au vu des premiers termes (et on le prouve alors facilement par récurrence double), ou bien on applique le cours que l'on connaît bien [10] sur les récurrences doubles. Bref, on trouve $D_n = \cos(n\alpha)$.
- CCINP 2010 (PSI) : Soit f l'application qui à tout $P \in \mathbb{R}[X]$ associe $Q \in \mathbb{R}[X]$ tel que $Q(x) = \displaystyle\int_x^{x+1} \widetilde{P}(t)dt$ pour tout $x \in \mathbb{R}$.
  1. Montrer que P induit un endomorphisme g de $\mathbb{R}_n[X]$.
  2. Calculer le déterminant de g.

  Solution : La matrice dans la base canonique est triangulaire...

Proposition 15 — Déterminant de Vandermonde

Soient $\lambda_1, ..., \lambda_n \in \mathbb{K}$. On a alors

$$V_n(\lambda_1, ..., \lambda_n) := \begin{vmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \vdots & \vdots & \vdots \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (\lambda_j - \lambda_i)$$

9. Les autres, ne lisez pas ces inepties !
10. Huhu !

PREUVE : Notons dès maintenant que si deux des λ_i sont égaux, alors deux colonnes sont égales, donc la matrice est de rang $< n$, donc son déterminant est nul (et la formule de l'énoncé est bien vérifiée !). On va donc supposer dans la suite que tous les λ_i sont distincts deux à deux.
On fixe $\lambda_1, ..., \lambda_{n-1}$ et on s'intéresse à $\varphi : \mu \mapsto V_n(\lambda_1, ..., \lambda_{n-1}, \mu)$. Il s'agit d'une application polynomiale de degré majoré par $n-1$. Son coefficient dominant est $V_{n-1}(\lambda_1, ..., \lambda_{n-1})$, et possède pour racines (au moins) $\lambda_1, ..., \lambda_{n-1}$. Comme il y en a autant que son degré, on les a toutes, donc $\varphi(\mu) = (\mu - \lambda_1)...(\mu - \lambda_{n-1})V_{n-1}$. On montre alors par récurrence la formule de l'énoncé. ■

REMARQUE : Ainsi, $V_n(\lambda_1, ..., \lambda_n) \neq 0$ si et seulement les λ_i sont distincts deux à deux. On peut le voir également (pour le sens moins clair) en supposant les λ_i distincts : l'application $\Phi : P \in \mathbb{K}_{n-1}[X] \mapsto (P(\lambda_1), ..., P(\lambda_n))$ est alors injective donc bijective, donc sa matrice entre les bases canoniques des espaces en jeu est inversible.

PROPOSITION 16 — Déterminants calculés par blocs

Pour une matrice diagonale par blocs, on peut écrire (pour deux blocs, mais aussi pour n) : $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ 0 & B \end{pmatrix}$, dont on tire sans mal : $\det \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det(A)\det(B)$.

Exercice 30. *Montrer que pour une matrice triangulaire par blocs* $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, *on a* $\det(M) = \det(A)\det(C)$.

On pourra commencer par traiter le cas où A n'est pas inversible. Lorsque A est inversible, on pourra chercher une factorisation comme dans la proposition précédente.

3 Polynômes et fractions rationnelles

Il n'y a a priori rien de nouveau dans ce qui suit. Il s'agit pour vous d'avoir un « texte de référence » que vous pouvez consulter en cas de doute sur un résultat ou une technique.

3.1 Rappels sur $\mathbb{K}[X]$

Commençons par une définition des plus précises...

DÉFINITION 18 — *L'algèbre* $\mathbb{K}[X]$

C'est une $\mathbb{K}$-algèbre ($\mathbb{K}$-espace vectoriel contenant $\mathbb{K}$, muni d'un produit interne, dans laquelle on calcule sans états d'âmes...), qui contient un objet X tel que $(1, X, ..., X^n, ...)$ est une base de $\mathbb{K}[X]$.

REMARQUE : Tout comme $\mathbb{C}$, on peut/va se contenter de cette présentation non constructive...
FAIT : Contrairement à toute attente, on a en général :

$$(p_0 + p_1X + \cdots + p_nX^n)(q_0 + q_1X + \cdots + q_nX^n) \neq p_0q_0 + p_1q_1X + \cdots + p_nq_nX^n.$$

DÉFINITION 19 — *Degré, valuation, dérivation*

Si $P = p_0 + p_1X + \cdots + p_nX^n \neq 0$, le **degré** de P est le plus grand k tel que $p_k \neq 0$, et la **valuation** de P est le plus petit k tel que $p_k \neq 0$ ($\deg(0) = -\infty$ et $\text{val}(0) = +\infty$ par convention). Les polynômes de degré majoré par n constituent un sous-espace noté $\mathbb{K}_n[X]$. Avec les notations précédentes, le polynôme dérivé de P, noté P' ou $D(P)$, est $p_1 + 2p_2X + np_nX^{n-1} = \sum_{k=1}^{n} kp_kX^{k-1}$.

THÉORÈME 14 — *Division euclidienne*

Si $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, alors il existe un unique couple $(P, Q) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$, avec $\deg(R) < \deg(B)$.

3.2 Racines d'un polynôme

Définition 20 — *Évaluation, racines d'un polynôme*

Si $P = p_0 + p_1 X + \cdots + p_n X^n \in \mathbb{K}[X]$ et $u \in \mathcal{A}$, avec $\mathcal{A}$ une $\mathbb{K}$-algèbre, l'évaluation de P en u est $\widetilde{P}(u) := p_0 + p_1 u + \cdots + p_n u^n \in \mathcal{A}$. On dit que $\alpha \in \mathbb{K}$ est **racine** de P lorsque $\widetilde{P}(\alpha) = 0$.

Une conséquence importante du théorème de division euclidienne est l'équivalence entre : « α est racine de P », et « $X - \alpha$ divise P » (l'un des sens étant trivial !). Il se peut qu'une plus grosse puissance de $X - \alpha$ divise P : on dit alors que α est racine multiple de P.

Définition 21 — *Multiplicité d'une racine*

Si α est racine de P, la **multiplicité** de α comme racine de P est le plus grand entier k tel que $(X - \alpha)^k$ divise P.

On se souvient que pour les « racines doubles » des polynômes de second degré, dans les petites classes, le graphe du trinôme avait une tangente horizontale en la racine double... Ça n'a pas changé ! Toujours pour ces trinômes, la dérivée seconde était non nulle. **On retient donc** : pour une racine double, $P(\alpha) = P'(\alpha) = 0$ et $P''(\alpha) \neq 0$. Le résultat qui suit ne fait que prolonger cela...

Théorème 15 — *Caractérisation de la multiplicité*

La multiplicité de α racine de P est le plus petit $k \in \mathbb{N}^*$ tel que $P^{(k)}(\alpha) \neq 0$.

Preuve : Admis, mais si vous avez des états d'âme : dans un sens, le fait que $(X-\alpha)^k$ divise P nous assure via la formule de Leibniz que $P^{(i)}(\alpha) = 0$ pour tout $i < \alpha$. Dans l'autre, utiliser la formule de Taylor (algébrique). ■

Mais peut-être qu'il y a eu un (ou deux ?) moment(s) de flottement en lisant la preuve précédente ?

Théorème 16 — *Formule de Leibniz*

Si $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$, alors :

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Preuve : Simple récurrence (contrairement au théorème d'analyse, il n'y a pas de dérivabilité à supposer/établir). ■

Théorème 17 — *Formule de Taylor algébrique*

Si $P \in \mathbb{K}[X]$ est de degré $\leqslant n$ et $a \in \mathbb{K}$, alors :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X - a)^k,$$

ou encore :

$$P(X + a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k.$$

Preuve : Pour la première version : P peut se décomposer dans la base (famille échelonnée) $(1, (X-a), ..., (X-a)^n)$. Il reste à calculer $((X-a)^n)^{(i)}(a)$. Pour la seconde : la formule du binôme permet de l'établir pour $P = X^n$, et on termine par linéarité (avec un peu de soin tout de même).
Dès qu'on a prouvé une des deux formulations, l'autre tombe bien entendu par application de la première à $Q = P(X + a)$ ou bien $Q = P(X - a)$ (on parle de composée (« P de $X - a$ » ou « P rond $X - a$ »), pas de produit !). ■

Exercice 31. *Donner la multiplicité de la racine 1 dans les polynômes suivants :*

1. $X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1$;
2. $X^{2n} - n^2 X^{n+1} + 2(n^2-1)X^n - n^2 X^{n-1} + 1$.

Théorème 18 — *Degré et nombre de racines*

Si $\alpha_1, ..., \alpha_k$ sont des racines distinctes de $P \neq 0$, de multiplicité $n_1, ..., n_k$, alors P est divisible par $(X-\alpha_1)^{n_1}...(X-\alpha_k)^{n_k}$. Corollairement, $\deg(P) \geqslant n_1 + \cdots + n_k$.

Conséquences souvent utilisées (sous ces diverses formulations) :
- Si $P \neq 0$ possède n racines distinctes, alors P est de degré au moins n.
- Si P possède n racines distinctes, alors P est nul ou est de degré au moins n.
- Si P possède une infinité de racines, alors P est nul.
- Si P est de degré au plus n et possède au moins $n+1$ racines distinctes, alors il est nul.

3.3 Lagrange

On commence par un résultat d'une grande profondeur... et dont on peut se souvenir quand on confond n, $n-1$ et $n+1$...

Fait : Par deux points distincts, on peut faire passer une droite !

Pour le problème qui nous intéresse, cela se traduirait :
Si $x_1, x_2, y_1, y_2 \in \mathbb{R}$ avec $x_1 \neq x_2$, alors il existe un (unique) polynôme P de degré au plus 1 tel que $P(x_1) = y_1$ et $P(x_2) = y_2$. Bref :

Interpolation en DEUX points $\Longrightarrow$ degré majoré par UN.

Théorème 19 — *Interpolation de Lagrange*

Si $x_1, ..., x_{n+1} \in \mathbb{K}$ sont distincts deux à deux et $y_1, ..., y_{n+1} \in \mathbb{K}$, alors il existe un unique polynôme P de degré au plus n tel que pour tout $i \in [\![1, n+1]\!]$, $P(x_i) = y_i$.

Preuve : On peut considérer l'application $\Phi \left\| \begin{array}{ccc} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}^{n+1} \\ P & \longmapsto & (P(x_1), ..., P(x_{n+1})) \end{array} \right.$, constater qu'elle est linéaire, montrer qu'elle est injective, et observer les dimensions.
Autre façon de procéder : on traite d'abord l'unicité. Pour l'existence, on peut exhiber directement un polynôme P qui convient. Pour cela, on peut commencer par traiter des cas simples (on donne les ensembles de couples (x_i, y_i)) :
- $\{(10,0); (999, \neq 0); (2048,0)\}$ (vous ne connaissez pas un polynôme de degré 2 nul en 10 et 2048 ?) ;
- $\{(10,0); (999,1); (2048,0)\}$;
- $\{(10,42); (999,0); (2048,0)\}$;
- $\{(10,42); (999,17); (2048,0)\}$;
- cas général...

■

Signalons qu'on parle d'interpolation car parfois on veut *interpoler* une fonction en $n+1$ points, c'est-à-dire trouver un polynôme qui coïncide avec cette fonction en des points imposés.

Exercice 32. *Déterminer l'ensemble des matrices engendré par la matrice diagonale $A = Diag(1, 2, ..., n)$ ainsi que ses puissances.*

Exercice 33. *Soient $x_1, ..., x_n$ des éléments distincts de $\mathbb{K}$, et $y_1, ..., y_n, z_1, ..., z_n \in \mathbb{K}$. Montrer qu'il existe un unique polynôme de degré au plus $2n-1$ tel que pour tout $i \in [\![1, n]\!]$, $P(x_i) = y_i$ et $P'(x_i) = z_i$.*

3.4 Factorisation en produit d'irréductibles

Les polynômes irréductibles jouent dans $\mathbb{K}[X]$ le rôle que les nombres premiers jouent chez les entiers : « on ne peut pas les écrire comme des produits ». Ben en fait si : $7 = 7.1 = (-7).(-1)$. De même, $X - 3 = 1.(X-3) = 3.(X/3 - 1) = \cdots$ Il convient donc de préciser le « on ne peut pas l'écrire comme un produit, sauf de façon triviale ».

Définition 22 — *Polynômes irréductibles*

Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible** lorsqu'il n'existe pas de décomposition $P = AB$ avec A et B deux polynômes non constants.

Remarques : Pour qu'un polynôme de degré $\geqslant 2$ soit irréductible, il est **nécessaire** qu'il ne possède pas de racines, mais ce n'est pas **suffisant** : vu comme polynôme réel, $(X^2+1)(X^2+2)$ n'a pas de racine, mais n'est pas irréductible !

Théorème 20 — *Factorisation en produits d'irréductibles*

Tout polynôme peut se décomposer comme produit d'irréductibles. De plus, si on impose aux irréductible P_i d'être unitaires, il y a unicité (à l'ordre près) de la décomposition sous la forme $\lambda P_1 ... P_n$.

Preuve : Comme dans $\mathbb{N}$ (pour l'existence) : par récurrence avec prédécesseurs (sur le degré). Pour l'unicité c'est plus délicat (ne serait-ce qu'à énoncer !) ; passons... ■

Définition 23 — *Polynômes scindés*

Un polynôme est dit **scindé** lorsqu'il s'écrit comme produit d'irréductibles de degré 1.

On a vu que $P = (X^2+1)(X^2+2)$ n'est pas scindé dans $\mathbb{R}[X]$, mais il l'est sur $\mathbb{C}$ puisque :

$$P = (X-i)(X+i)(X-i\sqrt{2})(X+i\sqrt{2}).$$

Théorème 21 — *Irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$*

- Dans $\mathbb{C}[X]$, tout polynôme est scindé (ou encore : tout polynôme non constant possède une racine).
- Dans $\mathbb{R}[X]$, les irréductibles sont les polynômes de degré $\leqslant 1$, ainsi que ceux de degré deux sans racine réelle.

Remarques :
- Dans $\mathbb{Q}[X]$ c'est bien plus compliqué ! Il y a des irréductibles de tous degrés : par exemple X^2+2, X^2-2 ou X^3-2...
- La connaissance des racines complexes (et leur multiplicité) permet de factoriser effectivement un polynôme complexe en produit d'irréductibles.
- Pour la factorisation dans $\mathbb{R}[X]$, on peut regrouper les racines complexes conjuguées.

Exercice 34. *Montrer que si P est un polynôme réel admettant pour racine $\alpha \in \mathbb{C}\setminus\mathbb{R}$, alors $\overline{\alpha}$ est également racine de P, de même multiplicité.*

Exemple : Soit $n \geqslant 1$. On a alors $X^n - 1 = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{2ik\pi/n}\right)$ sur $\mathbb{C}$. Sur $\mathbb{R}$, le regroupement des racines dépend de la parité de n. Si n est pair par exemple, alors 1 et -1 sont les racines réelles, et il reste $n-2$ racines non réelles conjuguées qu'on regroupe par deux (après avoir fait un petit dessin) pour trouver :

$$X^{2p} - 1 = (X-1)(X+1)\prod_{k=1}^{p-1}\left(X^2 - 2\cos\left(\frac{k\pi}{p}\right)X + 1\right).$$

Théorème 22 — *Relations coefficients-racines – aka « théorème du poulpe »*

Si $P = a_0 + a_1X + \cdots + a_nX^n$ ($a_n \neq 0$) a pour racines (comptées avec leur multiplicités) $x_1, ..., x_n$, alors la forme développée de $P = a_n(X-x_1)...(X-x_n)$ fournit n relations entre les a_i et les x_i.

Et NON, elles ne sont volontairement pas données dans l'énoncé...
Exemple : En observant le coefficient de X^{n-1} et le coefficient constant, on trouve :

$$x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad x_1x_2...x_n = (-1)^n\frac{a_0}{a_n}.$$

Exercice 35. *Soit $P = X^3 - 4X^2 + 2X - 1$. Montrer que P admet trois racines complexes distinctes, dont une seule est réelle. On les note x_1, x_2 et x_3.*
Calculer $x_1^2 + x_2^2 + x_3^2$ puis $x_1^3 + x_2^3 + x_3^3$. [On voudra bien trouver 12 et 43]

Exercice 36. (Centrale) *Calculer* $\displaystyle\prod_{k=1}^{n-1}\frac{1+\mathrm{e}^{2ik\pi/n}}{1-\mathrm{e}^{2ik\pi/n}}$.

Solution : Les $z_k = \dfrac{1+\mathrm{e}^{2ik\pi/n}}{1-\mathrm{e}^{2ik\pi/n}}$ vérifient $\left(\dfrac{z_k-1}{z_k+1}\right)^n = 1$, donc sont racines de $(X+1)^n-(X-1)^n$. Avec un peu d'attention, ce sont même LES racines de ce polynôme. Leur produit vaut donc

$$\pi = (-1)^{n-1}\frac{1-(-1)^n}{2n} = \frac{1+(-1)^{n-1}}{2n},$$

qui est nul comme prévu si n est pair.

3.5 Décomposition en éléments simples des fractions rationnelles (± H.-P.)

Le corps $\mathbb{K}(X)$ est pour l'anneau $\mathbb{K}[X]$ ce que $\mathbb{Q}$ est pour $\mathbb{Z}$. Ses habitants sont les quotients de polynômes, pour lesquels, « on fait les simplifications usuelles ». Le résultat suivant permettra entre autres choses d'intégrer les fractions rationnelles.

Théorème 23 — *Décomposition en éléments simples*

> Si $F \in \mathbb{K}(X)$, alors il existe une unique décomposition de F comme somme d'un polynôme et d'« éléments simples », c'est-à-dire des fractions de la forme $\dfrac{P}{Q^\alpha}$, avec Q irréductible et P tel que $\deg(P) < \deg(Q)$.

Preuve : Bof... Vous y tenez vraiment ? Pas moi. ■

En pratique les décompositions auront donc les têtes suivantes :

- Sur $\mathbb{C}$: si $F \in \mathbb{C}(X)$ a pour pôles (x_1,α_1), (x_2,α_2), …, (x_k,α_k), alors : $F = E + \sum_{i=1}^{k}\sum_{j=1}^{\alpha_i}\dfrac{\lambda_{i,j}}{(X-x_i)^j}$.
- Sur $\mathbb{R}$: Si $F \in \mathbb{R}(X)$ avec $F = \dfrac{P}{Q}$ (écriture irréductible), où Q est unitaire et de factorisation en produits d'irréductibles sur $\mathbb{R}$:

  $$\prod_{i=1}^{k}(X-x_i)^{\alpha_i}\prod_{i=1}^{r}(X^2+\lambda_i X+\beta_i)^{\rho_i},$$

  alors il existe un unique polynôme E, des réels $a_{i,j}$ ($1\leqslant i\leqslant k$ et $1\leqslant j\leqslant\alpha_i$), $b_{i,j}$ et $c_{i,j}$ ($1\leqslant i\leqslant r$ et $1\leqslant j\leqslant\rho_i$) tels que :

  $$F = E + \sum_{i=1}^{k}\Big(\sum_{j=1}^{\alpha_i}\frac{a_{i,j}}{(X-x_i)^j}\Big) + \sum_{i=1}^{r}\Big(\sum_{j=1}^{\rho_i}\frac{b_{i,j}X+c_{i,j}}{(X^2+\lambda_i X+\beta_i)^j}\Big).$$

Ne vous laissez pas impressionner par ces énoncés : en pratique ce sera assez simple !

Exemples : On va mettre en œuvre ici les différentes techniques qui doivent être maîtrisées :

- multiplication/évaluation en des racines ;
- utilisation de limites ;
- formule des résidus (H.P. : si α est pôle simple de $F = \dfrac{P}{Q}$, alors le coefficient de $\dfrac{1}{X-\alpha}$ dans la décomposition de F est $\dfrac{P(\alpha)}{Q'(\alpha)}$) ;
- développement limité ;
- (à la fin) évaluation en certains points.

1. On commence par l'indispensable $\dfrac{1}{X^2-1} = \dfrac{\frac{1}{2}}{X-1} - \dfrac{\frac{1}{2}}{X+1}$.
2. Si on note $j = \mathrm{e}^{2i\pi/3}$: $\dfrac{1}{X^3-1} = \dfrac{1}{3}\Big(\dfrac{1}{X-1} + \dfrac{j}{X-j} + \dfrac{\overline{j}}{X-\overline{j}}\Big)$.
3. Si $n \in \mathbb{N}^*$ et $\omega = \mathrm{e}^{2i\pi/n}$:

   $$\frac{1}{X^n-1} = \frac{1}{n}\sum_{k=0}^{n-1}\frac{\omega^k}{X-\omega^k}.$$

4. Si on note $\alpha = \mathrm{e}^{i\pi/4}$:
$$\frac{1}{X^4+1} = \frac{1}{4}\Big(\frac{\alpha}{X-\alpha} - \frac{\overline{\alpha}}{X+\overline{\alpha}} - \frac{\alpha}{X+\alpha} + \frac{\overline{\alpha}}{X-\overline{\alpha}}\Big)\cdot$$

5. $F = \dfrac{X+1}{(X-1)^2} = \dfrac{a}{X-1} + \dfrac{b}{(X-1)^2}$ (le degré de F est strictement négatif, donc sa partie entière est nulle). L'évaluation de $(X-1)^2F$ en 1 fournit $b=2$, et la limite de $t\widetilde{F}(t)$ en $+\infty$ fournit $b=1$:
$$\frac{X+1}{(X-1)^2} = \frac{1}{X-1} + \frac{2}{(X-1)^2}\cdot$$
On vérifie avec $\widetilde{F}(0)$.
On pouvait aussi noter que $X+1 = (X-1)+2$!

6. $G = \dfrac{2X^2+1}{(X-1)^2} = a + \dfrac{b}{X-1} + \dfrac{c}{(X-1)^2}$ (la partie entière est de degré nul, comme G). La limite de $\widetilde{G}$ en $+\infty$ fournit $a=2$. L'évaluation de $(X-1)^2G$ en 1 fournit $c=3$, et l'évaluation de G en 0 donne $1 = 2-b+3$, donc $b=4$:
$$\frac{2X^2+1}{(X-1)^2} = 2 + \frac{4}{X-1} + \frac{3}{(X-1)^2}\cdot$$
On vérifie avec $\widetilde{G}(-1)$.

7. $H = \dfrac{X^3+X+1}{(X-1)^2(X+1)^2} = \dfrac{a}{X-1} + \dfrac{b}{(X-1)^2} + \dfrac{c}{X+1} + \dfrac{d}{(X+1)^2}\cdot$ L'évaluation de $(X-1)^2H$ en 1 fournit $b = \dfrac{3}{4}$, et de même, $d = -\dfrac{1}{4}\cdot$ La limite de $t\widetilde{H}(t)$ en $+\infty$ fournit $a+c=1$, et l'évaluation en 0 donne $1 = -a + \dfrac{3}{4} + c - \dfrac{1}{4}$, puis $-a+c = \dfrac{1}{2}$, de sorte que $c = \dfrac{3}{4}$ et $a = \dfrac{1}{4}$:
$$H = \frac{\frac{1}{4}}{X-1} + \frac{\frac{3}{4}}{(X-1)^2} + \frac{\frac{3}{4}}{X+1} - \frac{\frac{1}{4}}{(X+1)^2}\cdot$$
On vérifie avec $\widetilde{H}(2)$ (surtout pas $\widetilde{H}(0)$: pourquoi ?).

8. $F = \dfrac{X^2+X+1}{(X^2+1)(X^2-1)} = \dfrac{aX+b}{X^2+1} + \dfrac{c}{X-1} + \dfrac{d}{X+1}\cdot$ Pour le calcul de a et b, on peut décomposer sur $\mathbb{C}$ puis regrouper les termes conjugués, mais il y a mieux : l'évaluation de $(X^2+1)F$ en i fournit $ai+b = \dfrac{i}{i^2-1} = -\dfrac{1}{2}i$, de sorte que $a = -\dfrac{1}{2}$ et $b=0$.

9. Encore une décomposition sur $\mathbb{R}$:
$$G = \frac{X+1}{(X^2+X+1)(X^2-X+1)} = \frac{aX+b}{X^2+X+1} + \frac{cX+d}{X^2-X+1}\cdot$$
L'évaluation de $(X^2+X+1)G$ en j racine de X^2+X+1 fournit :
$$aj+b = \frac{j+1}{j^2-j+1} = \frac{j+1}{-2j} = -\frac{1}{2}(j^3+j^2) = -\frac{1}{2}(-1-j-j-j^2) = \frac{1}{2}j$$
(on a utilisé au maximum la relation $j^2 = -1-j\ldots$), de sorte que[11] $a = \dfrac{1}{2}$ et $b=0$. En évaluant $(X^2-X+1)G$ en α racine de X^2-X+1, on obtient $c = -\dfrac{1}{2}$ et $d=1$, de sorte que :
$$G = \frac{\frac{1}{2}X}{X^2+X+1} + \frac{-\frac{1}{2}X+1}{X^2-X+1}\cdot$$
On vérifie avec $\widetilde{G}(0)$.

11. Liberté de $(1,j)$ dans $\mathbb{C}$ vu comme $\mathbb{R}$-espace vectoriel

10. Un dernier pour la route :

$$\begin{aligned} H &= \frac{2X^2 - X + 1}{(X-1)^3(X+1)^3} \\ &= \frac{a_1}{X-1} + \frac{a_2}{(X-1)^2} + \frac{a_3}{(X-1)^3} + \frac{b_1}{X+1} + \frac{b_2}{(X+1)^2} + \frac{b_3}{(X+1)^3}. \end{aligned}$$

On pose $K = (X-1)^3 H$: $\widetilde{K}(1+h) = a_3 + a_2 h + a_1 h^2 + o(h^2)$, et par ailleurs après calcul :

$$\widetilde{K}(1+h) = \frac{1}{8}\big(2(1+h)^2 - (1+h) + 1\big)(1+h/2)^{-3} = \frac{1}{4} + \frac{h^2}{16} + o(h^2),$$

de sorte que par unicité du développement limité, $a_3 = \dfrac{1}{4}$, $a_2 = 0$, et $a_1 = \dfrac{1}{16}$. On calcule les b_i en faisant un développement limité de $(X+1)^3 H$ au voisinage de -1, pour trouver finalement :

$$H = \frac{\frac{1}{16}}{X-1} + \frac{\frac{1}{4}}{(X-1)^3} + \frac{-\frac{1}{16}}{X+1} + \frac{-\frac{1}{8}}{(X+1)^2} + \frac{-\frac{1}{2}}{(X+1)^3}.$$

On vérifie avec $\widetilde{H}(0)$.

Exercice 37. *Décomposer en éléments simples sur $\mathbb{R}$ la fraction* $\dfrac{7}{(X+1)^7 - X^7 - 1}$.

Exercice 38. *Prouver :* $\displaystyle\int_0^1 \frac{dt}{1+t^3} = \frac{\pi\sqrt{3}}{9} + \frac{\ln 2}{3}$.

Exercice 39. *Décomposer en éléments simples dans $\mathbb{R}(X)$ la fraction* $F = \dfrac{2X+1}{(X^2+1)^2}$.