MP*1

Espaces vectoriels

Introduction

L'algèbre linéaire est la partie de l'algèbre la plus universellement utilisée en Mathématiques. Le contenu d'un cours sur le sujet est standard : espace vectoriel, dimension, applications linéaires, matrices, changement de bases, opérations élémentaires, déterminants, dualité (optionnel), systèmes linéaires.

Historiquement, l'algèbre linéaire a plusieurs sources : résolution de systèmes linéaires ou d'équations linéaires du type « interpolation », géométrie « des coordonnées », linéarisation des fonctions de plusieurs variables par l'introduction de la différentielle. Elle s'est développée dans l'ordre inverse de celui enseigné actuellement : la résolution de systèmes et les déterminants ont précédé les matrices, ces dernières ont précédé les applications linéaires et la notion d'espace vectoriel. Le lecteur qui aura le courage de lire les indications historiques qui concluent cette introduction verra que la synthèse actuelle, simple et efficace, est l'aboutissement d'un long effort. La présentation « moderne » de l'algèbre linéaire permet de dégager clairement deux notions importantes : celle d'équation linéaire (forme moderne des « systèmes ») et celle de dimension, qui est une première modélisation du « degré de liberté » en Mathématiques.

Comme presque toujours en Mathématiques, il y a en algèbre linéaire une tension entre l'aspect conceptuel et le calcul. Les notions d'espace vectoriel et d'application linéaire permettent de transférer à un contexte très large l'intuition acquise dans la géométrie du plan et de l'espace. Précisément, l'algèbre linéaire et la géométrie affine donnent une formulation générale des questions d'incidence. Elles ne s'occupent pas des problèmes métriques, dont la présentation moderne repose sur l'algèbre bilinéaire. Dans les situations concrètes, les outils calculatoires (matrices et déterminants) reprennent toute leur importance.

Ce texte et ceux qui le suivent ont un double but :

- permettre une révision de l'algèbre linéaire étudiée en première année,

- introduire un certain nombre d'objets et de résultats appartenant au « folklore » du sujet.

Ces documents ne constituent pas un cours complet. En particulier, on s'autorise une liberté à peu près totale quant à l'ordre : les applications linéaires sont largement utilisées avant d'avoir été réintroduites. Le lecteur est invité à se reporter à son cours de première année pour un exposé cohérent.

Dans toute la suite, $\mathbb{K}$ est un corps. [1]

1. Contrairement à ce que demande le programme officiel, il n'est pas pertinent de réduire l'étude aux cas où $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$. D'une part, le degré de généralité qu'offre la situation générale ne crée pas de complication à niveau élémentaire. D'autre part, l'algèbre linéaire sur les corps finis est à la base d'applications récentes et spectaculaires (cryptographie, codage) dont les premiers résultats sont tout à fait accessibles à un taupin.

Quelques repère chronologiques [2]

Comme signalé plus haut, la genèse de l'algèbre linéaire est embrouillée et passablement déconcertante pour le lecteur habitué aux exposés « modernes ».

- Les systèmes de deux équations linéaires à deux inconnues sont déjà pratiqués par les Babyloniens.

- Vers 1680, Leibniz étudie les systèmes linéaires et découvre les déterminants (d'ordre au plus 4). En 1750, Cramer définit en substance la signature d'une permutation par les inversions et obtient les formules de résolution d'un système linéaire qui portent son nom.

- Vers la même époque, l'étude des équations différentielles linéaires conduit Euler à la notion de combinaison linéaire ; c'est encore l'étude des équations différentielles qui amènera plus tard Cauchy à la notion d'indépendance linéaire.

- L'algorithme du pivot est exposé systématiquement par Gauss dans des travaux d'astronomie (1809). [3]

- L'étude des déterminants, initiée par Leibniz et Cramer, est poursuivie par Vandermonde et Lagrange (années 1770-1780). C'est Cauchy qui, le premier, démontre (par le calcul) les théorèmes de base sur les déterminants (1812). Les mathématiciens du dix-neuvième siècle utilisent abondamment les déterminants dans les problèmes « linéaires » et effectuent de très nombreux calculs.

- La notion de matrice apparaît dans divers problèmes (formes bilinéaires, « substitutions » linéaires) vers le milieu du dix-neuvième siècle. L'étude des matrices est alors envisagée sous un point de vue principalement calculatoire, ce qui n'empêche pas la découverte de résultats absolument non triviaux, notamment les diverses « réductions ». Quelques acteurs : Cayley (qui introduit la notion de matrice et le calcul matriciel), Cauchy, Jordan, Weierstrass (théorie spectrale et diverses réductions : diagonalisation orthogonale des matrices symétriques [4], « réduction de Jordan », « facteurs invariants »...).

- Les années 1870-1880 voient des tentatives de systématisation : Kronecker introduit les opérations élémentaires et donne une théorie complète des systèmes linéaires, Frobenius synthétise les résultats relatifs aux matrices et y ajoute de nombreux compléments.

- Quoiqu'il ait été perçu relativement tôt que les matrices et les déterminants permettent de développer une « géométrie en dimension n », l'approche « géométrique » de l'algèbre linéaire ne s'est imposé que très progressivement. Quelques précurseurs : Grassmann (1844, puis 1862), qui va bien au delà des notions de base en inventant l'« algèbre extérieure » ; Dedekind, dont la présentation de la théorie de Galois (1871), contient en germe la théorie de la dimension ; Peano (1888), qui dégage une première axiomatique des espaces vectoriels.

- Les travaux précédents restent isolés, jusqu'à ce qu'Emmy Noether développe, dans un article de 1921, [5] la présentation actuelle de l'algèbre linéaire

2. Lecture tout à fait facultative.
3. Cet algorithme semble avoir été connu des Chinois dès le deuxième siècle avant notre ère !
4. En liaison avec la recherche des « axes principaux » des coniques et quadriques.
5. Dans un contexte plus favorable : les travaux de Hilbert avaient imposé la « méthode axiomatique ».

(dans le cadre des modules, plus général que celui des espaces vectoriels). L'exposé de Noether est popularisé par Van der Waerden dans le livre d'algèbre le plus influent du vingtième siècle (« Moderne Algera », 1931).

1 Familles libres, liées, génératrices, bases

La notions de liberté, géométriquement intuitive, est la traduction en algèbre linéaire de la non-redondance. Rappelons les points suivants.

- Une sous-famille d'une famille libre est libre.

- Une famille est libre si et seulement si chacune de ses sous-familles finies est libre.

- Dire que la famille $(e_i)_{i\in I}$ est liée, c'est dire qu'il existe i_0 tel que e_{i_0} soit combinaison linéaire des e_i pour i dans $I \setminus \{i_0\}$. Incidemment, lors de la vérification de ce dernier point on est amené à diviser par un scalaire non nul, donc à utiliser que $\mathbb{K}$ est un corps.

Exemples fonctionnels de familles libres

Il est assez courant d'avoir à vérifier la liberté de familles de fonctions. Voici deux exemples simples, fondés sur l'utilisation de propriétés locales.

1. Soit E le $\mathbb{R}$-espace vectoriel $\mathbb{R}^{[0,1]}$. Pour α dans $\mathbb{R}^{+*}$, soit φ_α l'élément de E défini par
$$\forall x \in [0,1], \qquad \varphi_\alpha(x) = \sin(x^\alpha)$$
Pour tout n, on a
$$\varphi_\alpha(x) \underset{x\to 0}{\sim} x^\alpha$$
Le fait que les comportements des φ_α en 0 soient hiérarchisés de la sorte implique que $(\varphi_\alpha)_{\alpha\in\mathbb{R}^{+*}}$ est une famille libre d'éléments de E . En effet, si $0 < \alpha_1 < \cdots < \alpha_n$, si $\lambda_1, \ldots, \lambda_n$ sont des réels tels que
$$\forall x \in [0,1], \qquad \sum_{k=1}^{n} \lambda_k \varphi_{\alpha_k}(x) = 0,$$
on obtient, en divisant par x^{α_1} et en faisant tendre x vers 0, $\lambda_1 = 0$. Répétant cet argument, on voit que tous les λ_i sont nuls.
2. Posons, pour a dans $\mathbb{R}$:
$$\forall x \in \mathbb{R}, \qquad f_a(x) = |x-a|.$$
Alors $(f_a)_{a\in\mathbb{R}}$ est une famille libre de $\mathbb{R}^\mathbb{R}$. En effet, si tel n'était pas le cas, on aurait a tel que f_a soit combinaison linéaire des f_b pour b dans $\mathbb{R} \setminus \{a\}$. Absurde en examinant la dérivabilité en a.

Exercice 1. *Soit f la fonction définie sur $\mathbb{R}^+$ par :*
$$\forall x \in \mathbb{R}^+, \qquad f(x) = \ln(1+x).$$
Pour n dans $\mathbb{N}^*$, soit f_n l'itérée n-ième de f. Montrer que $(f_n)_{n\geq 1}$ est une famille libre du $\mathbb{R}$-espace $E = \mathbb{R}^{\mathbb{R}^+}$.

Exercice 2. *Si $a \in \mathbb{R}$, soit :*

$$\begin{array}{cccc} \varphi_a & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & \arctan(x+a) \end{array}$$

Est-ce que $(\varphi_a)_{a\in\mathbb{R}}$ est une famille libre de $E = \mathbb{R}^{\mathbb{R}}$?

Rappelons qu'une famille de vecteurs d'un espace vectoriel est une base si elle est libre et génératrice, ce qui permet de définir la notion de *coordonnées d'un vecteur dans une base*. Les espaces $\mathbb{K}^n$, $\mathbb{K}[X]$, $\mathbb{K}_n[X]$, $\mathcal{M}_{m,n}(\mathbb{K})$ portent des bases privilégiées, dites *canoniques*. [6]

Rappelons également que les combinaisons linéaires considérées en algèbre sont presque nulles, i.e. à support fini. Exemple : si X est un ensemble, l'ensemble $\mathbb{K}^X$ des fonctions de X dans $\mathbb{K}$ est naturellement un $\mathbb{K}$-espace vectoriel. Si x est dans X, soit δ_x la fonction indicatrice du singleton $\{x\}$. La famille $(\delta_x)_{x\in X}$ est clairement libre, mais le sous-espace qu'elle engendre n'est pas $\mathbb{K}^X$ si X est infini : c'est le sous-espace $\mathbb{K}^{(X)}$ des fonctions presque nulles de X dans $\mathbb{K}$.

Exemples polynomiaux de familles libres, de bases

1. *Familles à degrés distincts, échelonnés*
   Une famille de polynômes non nuls à degrés deux à deux distincts est libre. Cet énoncé immédiat peut être utilisé sans démonstration (mais en étant clairement formulé). Un corollaire est qu'une famille $(P_k)_{0\leq k\leq n}$ (resp. $(P_k)_{k\in\mathbb{N}}$) d'éléments de $\mathbb{K}[X]$ telle que, pour tout k, P_k soit de degré k est une base de $\mathbb{K}_n[X]$ (resp. de $\mathbb{K}[X]$).

2. *Base de Lagrange*
   Soient $a_1, \ldots, a_n$ des éléments de $\mathbb{K}$ deux à deux distincts. Pour k dans $\{1, \ldots, n\}$, soit
   $$L_k = \prod_{\substack{1\leq i\leq n \\ i\neq k}} \left(\frac{X - x_i}{x_k - x_i}\right).$$
   Alors $(L_k)_{1\leq k\leq n}$ est une base de $\mathbb{K}_{n-1}[X]$. La décomposition de l'élément P de $\mathbb{K}_{n-1}[X]$ sur cette base est la *formule d'interpolation de Lagrange* :
   $$P = \sum_{k=1}^{n} P(a_k)\ L_k.$$
   Elle permet de reconstituer P à partir des valeurs $P(a_k)$.

3. *Formule de Taylor*
   Soient n dans $\mathbb{N}$, a un élément de $\mathbb{K}$. Les polynômes $(X-a)^k$, $k \in \mathbb{N}$ forment une base de $\mathbb{K}[X]$ (degrés échelonnés). Cherchons, si P est dans $\mathbb{K}[X]$, la décomposition de P sur cette base. Écrivons, en notant n le degré de P :
   $$P = \sum_{j=0}^{n} \lambda_j (X-a)^j, \qquad (\lambda_0, \ldots, \lambda_n) \in \mathbb{K}^{n+1}.$$

6. Attention, la notion de base canonique n'a pas de sens dans un $\mathbb{K}$-espace vectoriel E « général ».

En dérivant k fois ($0 \leq k \leq n$) et en évaluant en a, on obtient $k!\ \lambda_k = P^{(k)}(a)$. En supposant $\mathbb{K}$ de caractéristique nulle, on obtient la *formule de Taylor* :

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

Liberté d'une famille de vecteurs propres

Soient E un $\mathbb{K}$-espace vectoriel, u dans $\mathcal{L}(E)$, λ dans $\mathbb{K}$ et x dans E. On dit que x est vecteur propre de u associé à λ si $x \neq 0$ et si

$$u(x) = \lambda x,$$

autrement dit si la droite $\mathbb{K}x$ est stable par u et si u induit sur cette droite l'homothétie de rapport λ.

Théorème 1. *Soient E un $\mathbb{K}$-espace vectoriel, u dans $\mathcal{L}(E)$, $(x_i)_{i\in I}$ une famille d'éléments de E constituée de vecteurs propres de u associés à des valeurs propres deux à deux distinctes. Alors $(x_i)_{i\in I}$ est libre.*

Nous en donnons deux démonstrations, toutes deux instructives.

Preuve 1. Montrons, par récurrence sur $n \in \mathbb{N}^*$, l'assertion $\mathcal{A}_n$ suivante : « pour tout u de $\mathcal{L}(E)$, toute famille $(x_i)_{1\leq i\leq n}$ de vecteurs propres de u associés à des valeurs propres deux à deux distinctes est libre ». L'assertion $\mathcal{A}_1$ est triviale. Supposons $n \geq 2$, $\mathcal{A}_{n-1}$ démontrée et adoptons les notations de $\mathcal{A}_n$, en notant λ_i la valeur propre de u associée à x_i. Soit $(\alpha_1, \ldots, \alpha_n)$ une famille de scalaires telle que

$$(1) \qquad \sum_{i=1}^{n} \alpha_i x_i = 0.$$

En appliquant u à cette relation, il vient

$$(2) \qquad \sum_{i=1}^{n} \alpha_i \lambda_i x_i = 0.$$

En combinant les relations (1) et (2), il vient :

$$\sum_{i=1}^{n-1} (\lambda_i - \lambda_n)\alpha_i x_i = 0.$$

Les $\lambda_i - \lambda_n$ sont non nuls. On en déduit en appliquant $\mathcal{A}_{n-1}$ que $\alpha_1, \ldots, \alpha_{n-1}$ sont nuls. Revenant à (1), on voit que α_n est nul ce qui achève la démonstration.

Preuve 2. On part de (1). En appliquant à cette relation les $u^j, j \in \mathbb{N}$ et en faisant des combinaisons linéaires, on obtient

$$\forall P \in \mathbb{K}[X], \qquad \sum_{i=1}^{n} \alpha_i P(\lambda_i) x_i = 0.$$

Choisissant $P = \prod_{\substack{1\leq i\leq n,\\ i\neq j}} (X - x_i)$, il vient $\lambda_j = 0$.

Exemple *Fonctions exponentielles*

Soient I un intervalle non trivial de $\mathbb{R}$, E le $\mathbb{C}$-espace vectoriel des fonctions de classe C^∞ de I dans $\mathbb{C}$, D l'endomorphisme de dérivation sur E. Pour λ dans $\mathbb{C}$ soit e_λ l'élément de E défini par

$$\forall x \in I, \qquad e_\lambda(x) = \exp(\lambda x).$$

Pour tout λ, e_λ est vecteur propre de D associé à la valeur propre λ. Le théorème 1 montre que $(e_\lambda)_{\lambda \in \mathbb{C}}$ est libre.

Exercice 3. *Pour θ dans $\mathbb{C}$, soit $u_\theta = (\theta^n)_{n \geq 0}$. Démontrer la liberté de la famille des suites géométriques $(u_\theta)_{\theta \in \mathbb{C}}$ dans $\mathbb{C}^{\mathbb{N}}$.*

Exercice 4. *Soient I un intervalle non trivial de $\mathbb{R}$ et, pour λ dans $\mathbb{R}^+$, c_λ la fonction de I dans $\mathbb{R}$ définie par*

$$\forall x \in I, \qquad c_\lambda(x) = \cos(\lambda x).$$

Montrer que $(c_\lambda)_{\lambda \in \mathbb{R}^+}$ est une famille libre de $\mathbb{R}^I$.

Exercice 5. *Montrer que $(\ln(p))_{p \in \mathcal{P}}$ est une famille libre du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.*

L'exemple ci-après n'est pas une application du théorème 1.

Exercice 6. *Lemme de Dedekind*

Soient $(M, .)$ un monoïde et $(\sigma_i)_{i \in I}$ une famille de morphismes distincts de $(M, .)$ dans $(K^*, \times)$. Montrer que $(\sigma_i)_{i \in I}$ est une famille libre de K^M. Retrouver l'exemple des fonctions exponentielles dans le cas $I = \mathbb{R}$ et l'exercice précédent.

2 Espaces de dimension finie

Rappelons que l'on définit la notion d'espace vectoriel de dimension finie avant celle de dimension : le $\mathbb{K}$-espace vectoriel E est dit de dimension finie s'il admet une famille génératrice finie. Pour montrer qu'un tel espace admet une base finie, on s'appuie sur le résultat suivant.

Théorème 2. *Soit $(x_i)_{1 \leq i \leq n}$ une famille génératrice de E. Soit I une partie de $\{1, \ldots, n\}$ telle que $(x_i)_{i \in I}$ soit libre. Il existe alors une partie J de $\{1, \ldots, n\}$ contenant I telle que $(x_i)_{i \in J}$ soit une base de E.*

La démonstration consiste simplement à choisir J de sorte que $(x_i)_{i \in J}$ soit libre et maximale pour l'inclusion. Ce théorème a deux corollaires utiles : le théorème de la base incomplète et le théorème de la base extraite.

On démontre que toutes les bases d'un espace vectoriel sont équipotentes à partir de l'énoncé suivant.

Théorème 3. *Si E admet une famille génératrice de cardinal n, toute famille de $n+1$ vecteurs de E est liée.*

Ce dernier résultat s'établit par récurrence. Deux approches sont possibles : l'algorithme du pivot ou le lemme d'échange de Steinitz. La première méthode est une des techniques les plus importantes en algèbre linéaire « effective », puisqu'elle donne une manière efficace de résoudre les systèmes linéaires (donc, par exemple, de déterminer les coordonnées d'un vecteur dans une base).

Le théorème entraîne la caractérisation des bases d'un espace de dimension finie n comme familles libres de n vecteurs, ou comme familles génératrices de n vecteurs.

Exemples et applications

1. *Extension des scalaires*

   Soient E un $\mathbb{C}$-espace de dimension n, $(e_1, \dots, e_n)$ une base de E. Par restriction des scalaires, E est un $\mathbb{R}$-espace vectoriel. Il est immédiat de vérifier que $(e_1, \dots, e_n, ie_1, \dots, ie_n)$ est une base de E comme $\mathbb{R}$-espace vectoriel. Ainsi
   $$\dim_{\mathbb{R}}(E) = 2 \dim_{\mathbb{C}} E.$$

   Cet exemple se généralise : si $\mathbb{F}$ est un surcorps de $\mathbb{K}$ de dimension finie $[\mathbb{F} : \mathbb{K}]$ comme $\mathbb{K}$-espace vectoriel et E un $\mathbb{F}$-espace vectoriel de dimension n, alors E est un $\mathbb{K}$-espace vectoriel de dimension $n\,[\mathbb{F} : \mathbb{K}]$.

2. *Une utilisation en théorie des corps*

   Soit $\mathbb{K}$ un corps fini. Nécessairement, $\mathbb{K}$ est de caractéristique non nulle (sinon $\mathbb{K}$ contiendrait un sous-corps isomorphe à $\mathbb{Q}$). Cette caractéristique est un nombre premier p (intégrité). Il s'ensuit que le sous-anneau premier de $\mathbb{K}$ est un corps isomorphe à $\mathbb{F}_p$. Notant d la dimension de $\mathbb{K}$ comme $\mathbb{F}_p$-espace vectoriel, $\mathbb{K}$ est de cardinal p^d.

   On a établi que le cardinal d'un corps fini est une puissance de nombre premier. Réciproquement, on peut démontrer que, si q est de la forme p^m avec p premier et m dans $\mathbb{N}^*$, il existe un corps de cardinal q et que deux corps de cardinal q sont isomorphes.

3. *Une utilisation en théorie des groupes*

   Soient p un nombre premier, $(G, +)$ un groupe abélien fini de neutre 0 tel que
   $$\forall g \in G, \qquad p.g = 0.$$

   Alors, il existe n dans $\mathbb{N}^*$ tel que G soit isomorphe au groupe additif $(\mathbb{Z}/p\mathbb{Z})^n$. Pour le voir, on munit G d'une structure d'espace vectoriel sur $\mathbb{F}_p$. Pour g dans G et k dans $\mathbb{Z}$, on observe que kg ne dépend que de la classe $\overline{k}$ de k modulo p. On peut donc définir
   $$\forall (k, g) \in \mathbb{F}_p \times G, \qquad \overline{k}g = kg.$$

   Cette multiplication externe fait bien de G un $\mathbb{F}_p$-espace vectoriel, l'addition étant la loi + initiale (la vérification des axiomes d'espace vectoriel est laissée au lecteur). Cet espace est de dimension finie n. Et G est isomorphe à $(\mathbb{F}_p)^n$ comme $\mathbb{F}_p$-espace vectoriel, donc comme groupe abélien.

Exercice 7. *Soit* $(x_1, \dots, x_n)$ *une famille génératrice du* $\mathbb{K}$*-espace vectoriel* E*. On pose*

$$I = \{i \in \{1, \dots, n\} \ ; \ x_i \notin \mathit{Vect}((x_1, \dots, x_{i-1})\}.$$

Que dire de $(x_i)_{i \in I}$ *?*

Exercice 8. *Soient* $P_1, \dots, P_4$ *des éléments de* $\mathbb{K}_3[X]$ *s'annulant en* 1*. La famille* $(P_i)_{1 \leq i \leq 4}$ *peut-elle être libre ?*

Exercice 9. *Montrer que* $\left(X^k(1-X)^{n-k}\right)_{0 \leq k \leq n}$ *est une base de* $\mathbb{K}_n[X]$*.*

Exercice 10. *Soient* $c_0, \dots, c_{n+1}$ *des éléments de* $\mathbb{C}$ *deux à deux distincts. Montrer que* $((X - c_i)^n)_{0 \leq i \leq n+1}$ *est une base de* $\mathbb{C}_n[X]$*, puis décomposer* 1 *sur cette base.*

Exercice 11. *Soit* V *un sous-espace vectoriel de dimension finie de* $\mathbb{K}[X]$*.*

a) Montrer qu'il existe une base de V *formée d'éléments de degrés deux à deux distincts.*

b) Montrer qu'il existe une base de V *formée d'éléments ayant tous le même degré.*

Exercice 12. *Démontrer la généralisation mentionnée à la fin de l'exemple 1.*

Exercice 13. *Soit* G *un groupe fini de neutre* e *tel que :*

$$\forall g \in G, \qquad g^2 = e.$$

Montrer que G *est abélien. En utilisant l'exemple 3 ci-dessus, qu'en déduit-on sur la structure de* G *?*

Exercice 14. *Soient* n *dans* $\mathbb{N}^*$*,* $\mathcal{P} = \{p_1, \dots, p_{n+1}\}$ *un ensemble de* $n+1$ *nombres premiers distincts,* $x_1, \dots, x_n$ *des éléments de* $\mathbb{N}^*$ *ayant tous leurs facteurs premiers dans* $\mathcal{P}$*. Montrer qu'il existe un sous-ensemble non vide* I *de* $\{1, \dots, n+1\}$ *tel que* $\prod_{i \in I} x_i$ *soit un carré parfait.*

Exercice 15. *Soient* P *et* Q *dans* $\mathbb{K}[X]$*. Montrer qu'il existe* U *dans* $\mathbb{K}[X, Y] \setminus \{0\}$ *tel que* $U(P, Q) = 0$*. On pourra montrer que, pour* n *assez grand, la famille* $(P^k Q^\ell)_{0 \leq k, \ell \leq n}$ *est liée.*

Exercice 16. *Soit* V *un sous-espace non nul de* $\mathbb{K}^n$ *On suppose que tout vecteur non nul de* V *a toutes ses coordonnées non nulles. Montrer que* V *est une droite.*

La théorie de la dimension a des applications surprenantes. Voici deux jolis exemples combinatoires. [7]

Exercice 17. *Soient* E *un ensemble fini de cardinal* n*,* $X_1, \dots, X_{n+1}$ *des parties de* E*. Montrer qu'il existe deux parties* I *et* J *de* $\{1, \dots, n+1\}$*, disjointes et non vides, telles que*

$$\bigcup_{i \in I} X_i = \bigcup_{j \in J} X_j.$$

On se placera dans le $\mathbb{Q}$*-espace vectoriel* $\mathbb{Q}^E$*, on considérera les indicatrices* 1_{X_j}*.*

7. La technique utilisée dans le second exemple est standard et se résume comme suit. Pour estimer le cardinal d'un ensemble fini S, on associe à chaque s de S un vecteur v_s d'un espace vectoriel E de dimension finie d. Si $(v_s)_{s \in S}$ est libre, on a nécessairement $|S| \leq d$.

Exercice 18. *L'espace $\mathbb{R}^n$ est muni de sa structure euclidienne canonique. On se donne p dans $\mathbb{N}^*$, α et β deux éléments de $\mathbb{R}^{+*}$, $a_1, \ldots, a_p$ dans $\mathbb{R}^n$ tels que :*

$$\forall (i,j) \in \{1, \ldots, p\}^2,\ i \neq j \Rightarrow \|a_i - a_j\| \in \{\alpha, \beta\}.$$

Pour j dans $\{1, \ldots, p\}$, la fonction f_j est définie par :

$$\forall x \in \mathbb{R}^n, \qquad f_j(x) = \left(\|x - a_j\|^2 - \alpha^2\right)\ \left(\|x - a_j\|^2 - \beta^2\right).$$

a) Montrer que $(f_1, \ldots, f_p)$ est une famille libre de $\mathcal{F}(\mathbb{R}^n, \mathbb{R})$.

b) Montrer la dimension du sous-espace de $\mathcal{F}(\mathbb{R}^n, \mathbb{R})$ engendré par $(f_1, \ldots, f_p)$ est majorée par $\dfrac{n^2+5n+4}{2}$. Qu'en déduit-on sur p ?

d) On suppose $n > 2$ et on considère l'ensemble X des vecteurs de $\mathbb{R}^n$ ayant 2 coordonnées égales à 1 et $n-2$ nulles. Déterminer le cardinal de X et l'ensemble des distances $\|x - x'\|$, $(x, x') \in X^2, x \neq x'$. Conclusion ?

La dimension infinie

L'axiome du choix permet de généraliser les résultats précédents. Il entraîne qu'un espace vectoriel E admet toujours une base, que deux bases de E sont équipotentes. Le caractère non constructif des démonstrations rend ces énoncés quelque peu chimériques. Il est en général impossible de produire une base d'un espace vectoriel de dimension infinie [8]. Exception : l'espace de polynômes $\mathbb{K}[X]$.

Exercice 19. *En utilisant le décomposition en éléments simples, donner une base du $\mathbb{C}$-espace $\mathbb{C}(X)$.*

En fait, l'algèbre linéaire « pure » en dimension infinie a peu d'applications : lorsqu'un espace de dimension infinie apparaît naturellement, il est souvent muni d'une structure additionnelle (par exemple d'une norme ou au moins d'une topologie compatible avec les opérations).

3 Calculs de dimension

Un espace vectoriel E peut être décrit de deux façons, qui conduisent toutes deux à des méthodes permettant d'en calculer la dimension.

- La première description est la donnée d'une famille génératrice. Si la famille est libre, c'est une base et la dimension de E est connue. Sinon, il faut « mesurer les redondances », ce qui peut se faire en extrayant une base.

Variante : E est donné comme image d'une application linéaire u. Si u est injective, la dimension de E est celle de la source de u. Sinon, on utilise le théorème du rang.

- La seconde description est la donnée d'une famille d'équations linéaires dont E est l'espace des solutions. Variante : E est donné comme le noyau d'une application linéaire définie sur un « sur-espace » de E.

8. Ainsi, l'axiome du choix assure l'existence d'une base de $\mathbb{R}$ comme $\mathbb{Q}$-espace vectoriel ; une telle famille est souvent nommée *base de Hamel*. Il est impossible d'expliciter une base de Hamel.

Ici encore le théorème du rang joue un rôle essentiel. L'idée clé est que la dimension d'un sous-espace vectoriel d'un espace de dimension n décrit par p équations linéaires indépendantes est $n-p$.

Les exemples ci-après utilisent la première technique. Nous verrons plus loin des applications de la seconde.

Exemples

1. *Dimension d'un produit*
   Soient E un $\mathbb{K}$-espace vectoriel de dimension m, F un $\mathbb{K}$-espace de dimension p, $(e_1,\dots,e_n)$ (resp. $(f_1,\dots,f_p)$) une base de E (resp. F). On vérifie sans difficulté que $((e_1,0),\dots,(e_n,0),(0,f_1),\dots,(0,f_p))$ est une base de $E\times F$. La dimension de $E\times F$ est donc $n+p$.
2. *Suites récurrentes linéaires*

   Fixons p dans $\mathbb{N}^*$, $(a_0,\dots,a_{p-1})$ dans $\mathbb{K}^p$. On vérifie immédiatement que l'ensemble E des suites $(u_n)_{n\geq 0}$ d'éléments de $\mathbb{K}$ telles que
   $$\forall n\in\mathbb{N},\qquad u_{n+p}=a_{p-1}u_{n+p-1}+\cdots+a_0u_n$$
   est un sous-espace de $\mathbb{K}^{\mathbb{N}}$. Manifestement, si $(x_0,\dots,x_{p-1})\in\mathbb{K}^p$, il existe une unique suite $(u_n)_{n\geq 0}$ de E telle que
   $$\forall i\in\{0,\dots,p-1\},\qquad u_i=x_i.$$
   L'application φ de E dans $\mathbb{K}^p$ qui à $(u_n)_{n\geq 0}$ associe $(u_0,\dots,u_{p-1})$ est donc une bijection de E sur $\mathbb{K}^p$. Comme φ est manifestement linéaire, c'est un isomorphisme de E sur $\mathbb{K}^p$. Donc E est de dimension p. [9]
3. *Polynômes homogènes de degré d dans $\mathbb{K}[X_1,\dots,X_n]$*
   Un polynôme de $\mathbb{K}[X_1,\dots,X_n]$ est dit *homogène de degré d* s'il est combinaison $\mathbb{K}$-linéaire des monômes $X^\alpha=\displaystyle\prod_{i=1}^n X_i^{\alpha_i}$ tels que $\sum_{i=1}^n\alpha_i=d$.
   Les monômes précédents forment une base de l'espace des polynômes homogènes de degré d de $\mathbb{K}[X_1,\dots,X_n]$. La dimension de cet espace est donc égale au nombre de ces monômes, c'est-à-dire au nombre de n-uplets $(\alpha_1,\dots,\alpha_n)$ de $\mathbb{N}^n$ tels que
   $$\sum_{i=1}^n\alpha_i=d,$$
   classiquement égal à $\binom{n+d-1}{d}$.
4. *Fonctions affines par morceaux associées à une subdivision*
   Soient $a=a_0<a_1<\cdots<a_n=b$ des réels et $\mathcal{A}$ l'ensemble des fonctions continues de $[a,b]$ dans $\mathbb{R}$ dont la restriction à chaque $[a_i,a_{i+1}]$ pour $0\leq i\leq n-1$ soit affine. On vérifie que $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{F}([0,1],\mathbb{R})$. Quelle est sa dimension ?

9. Cet argument se généralise à des relations de récurrence linéaires homogènes à coefficients non constants.

Un élément de $\mathcal{A}$ est défini par ses valeurs en $a_0, \ldots, a_n$, ces nombres pouvant être choisis arbitrairement. On en déduit que la dimension est $n+1$. La mise en forme de ce raisonnement est naturelle. On introduit l'application Φ de $\mathcal{A}$ dans $\mathbb{R}^{n+1}$ définie par

$$\forall f \in \mathcal{A}, \qquad \Phi(f) = (f(a_0), f(a_1), \ldots, f(a_n)).$$

L'application Φ est linéaire. Elle est clairement bijective. Donc $\mathcal{A}$ a même dimension que $\Phi(\mathcal{A}) = \mathbb{R}^{n+1}$.

Exercice 20. *Déterminer la dimension de l'espace des matrices symétriques de $\mathcal{M}_n(\mathbb{K})$. Même question avec l'espace des matrices antisymétriques.*

Exercice 21. *Vérifier que l'ensemble des matrices M de $\mathcal{M}_n(\mathbb{C})$ telles que $\overline{{}^tM} = M$ est un sous-espace vectoriel réel (mais pas complexe) de $\mathcal{M}_n(\mathbb{C})$. En donner la dimension.*

Exercice 22. *Quelle est la dimension du sous-espace de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ engendré par les fonctions : $x \mapsto \sin(x+a)$ pour a dans $\mathbb{R}$?*

Exercice 23. *Soit n dans $\mathbb{N}^*$. Pour $1 \leq k \leq n$, on note f_k la fonction définie sur $\mathbb{R}$ par :*

$$\forall x \in \mathbb{R}, \qquad f_k(x) = \sin(kx)\cos((n-k)x).$$

Quel est le rang de $(f_k)_{1 \leq k \leq n}$?

Exercice 24. *Soient E et F deux $\mathbb{K}$-espaces de dimension finie, $(e_i)_{1 \leq i \leq n}$ une base de E, $(f_j)_{1 \leq j \leq p}$ une base de F. Quelle est la dimension du sous-espace de $E \times F$ engendré par les vecteurs :*

$$(e_i, f_j), \qquad 1 \leq i \leq n, \quad 1 \leq j \leq p\,?$$

Exercice 25. *Soient $a = a_0 < a_1 < \cdots < a_n = b$ des réels et $\mathcal{S}$ l'espace des fonctions de classe C^2 de $[a, b]$ dans $\mathbb{R}$ dont la restriction à chaque $[a_i, a_{i+1}]$ pour $0 \leq i \leq n-1$ est un polynôme de degré ≤ 3. Quelle est la dimension de $\mathcal{S}$?*

Exercice 26. *Soient $E_1, \ldots, E_r$ et F des $\mathbb{K}$-espaces vectoriels de dimension finie. Déterminer la dimension de l'espace des applications r-linéaires du $\mathbb{K}$-espace $E_1 \times \cdots \times E_r$ dans le $\mathbb{K}$-espace F.*

Exercice 27. *On suppose $\mathbb{K}$ fini de cardinal q. Soit n dans $\mathbb{N}^*$. Si P est un élément de $\mathbb{K}[X_1, \ldots, X_n]$, on pose*

$$V_P = \{(x_1, \ldots, x_n) \in \mathbb{K}^n \; ; \; P(x_1, \ldots, x_n) = 0\}.$$

On rappelle que le degré du monôme $\displaystyle\prod_{i=1}^{n} X_i^{\alpha_i}$ est $\displaystyle\sum_{i=1}^{n} \alpha_i$, et qu'on appelle de gré d'un élément de $\mathbb{K}[X_1, \ldots, X_n] \setminus \{0\}$ le degré maximal d'un monôme apparaissant dans P.

a) Montrer que si P est de degré au plus $q-1$ et $V_P = \mathbb{K}^n$, alors $P = 0$.

b) Soit X une partie de $\mathbb{K}^n$ telle que $|X| < \binom{n+q-1}{q-1}$. Montrer qu'il existe P dans $\mathbb{K}[X_1, \ldots, X_n]$ tel que $V_P \neq \mathbb{K}^n$ et $X \subset V_P$.

Exercice 28. *Soient n dans $\mathbb{N}^*$, d dans $\mathbb{N}$. Notons $\mathcal{H}_{n,d}$ le sous-espace de $\mathbb{R}[X_1, \dots, X_n]$ constitué des polynômes homogènes de degré d. Soit Δ l'opérateur laplacien sur $\mathbb{R}[X_1, \dots, X_n]$.*

a) Soit P dans $\mathcal{H}_{n,d}$. On écrit

$$P = \sum_{j=0}^{d} P_j(X_1, \dots, X_{n-1}) {X_n}^j,$$

où, pour tout j, P_j est dans $\mathbb{R}[X_1, \dots, X_{n-1}]$. À quelle condition sur les P_j le polynôme P est-il harmonique ? En déduire la dimension de $Ker(\Delta) \cap \mathcal{H}_{n,d}$.

Exercice 29. *Soient d dans $\mathbb{N}$, $\mathbb{R}[X,Y]_d$ le sous-espace de $\mathbb{R}[X,Y]$ constitué des polynômes homogènes de degré d.*

a) Montrer que, si $d \geq 2$, l'image de $\mathbb{R}[X,Y]$ par l'opérateur laplacien Δ est $\mathbb{R}[X,Y]_{d-2}$. Montrer que $(X^2+Y^2)\ \mathbb{R}[X,Y]_{d-2}$ et le sous-espace de $\mathbb{R}[X,Y]_d$ des polynômes harmoniques sont deux sous-espaces supplémentaires de $\mathbb{R}[X,Y]_d$.

b) Montrer que, si P est dans $\mathbb{R}[X,Y]_d$, P s'écrit

$$\sum_{j=0}^{\lfloor \frac{d}{2} \rfloor} (X^2+Y^2)^j P_j$$

où, pour tout j, P_j est un polynôme harmonique de $\mathbb{R}[X,Y]_{d-2j}$.

c) Si P est dans $\mathbb{R}[X,Y]$, montrer qu'il existe un polynôme harmonique coïncidant avec P sur S^1. Généraliser ces résultats en dimension n.

4 Sous-espaces d'un espace de dimension finie

Les résultats de la section précédente entraînent le résultat suivant

Théorème 4. *Soient E un $\mathbb{K}$-espace vectoriel de dimension n et F un sous-espace de E. Alors F est de dimension finie $m \leq n$, l'égalité $m = n$ ayant lieu si et seulement si $E = F$.*

Une notion très utile reliée à ce résultat est celle de *base de E adaptée à F*. On appelle ainsi toute base $(e_1, \dots, e_n)$ de E telle que $(e_1, \dots, e_m)$ soit une base de F. Pour construire une telle base, on part d'une base de F, qui est une famille libre de E, ce qui permet de la compléter en une base de E. [10]

Exemple *Quelques dénombrements sur un corps fini*

L'algèbre linéaire sur un corps fini a des applications pratiques significatives (codes correcteurs d'erreurs). Introduisons le sujet par quelques problèmes de dénombrement. Soient $\mathbb{K}$ un corps fini de cardinal q, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$. On se propose de dénombrer :

- l'ensemble E ;

- pour $1 \leq m \leq n$, le nombre de familles libres $(e_1, \dots, e_m)$ de E^m ;

10. Attention, une base quelconque de E n'a pas de raison d'avoir le moindre rapport avec F. Prendre pour E le plan $\mathbb{R}^2$ usuel, pour F toute droite autre que les axes canoniques et considérer la base canonique de E.

- pour $1 \leq m \leq n$, le nombre de sous-espaces vectoriels de dimension m de l'espace E.

Comme est E est isomorphe comme $\mathbb{K}$-espace vectoriel à $\mathbb{K}^n$, en particulier équipotent à $\mathbb{K}^n$, $|E| = q^n$.

Dire que la famille $(e_1, \ldots, e_m)$ est libre, c'est dire que $e_1 \neq 0$, que $e_2 \notin \mathbb{K}e_1$, que $e_3 \notin \mathbb{K}e_1 \oplus \mathbb{K}e_2$, ..., que $e_m \notin \mathbb{K}e_1 \oplus \mathbb{K}e_2 \oplus \cdots \oplus \mathbb{K}e_{m-1}$. Il y a donc $q^n - 1$ choix pour e_1, $q^n - q$ choix pour e_2, ..., $q^n - q^{m-1}$ choix pour e_m. Le nombre de familles libres de m vecteurs est donc

$$\gamma_{n,m}(q) = \prod_{i=0}^{m-1} (q^n - q^i).$$

Le nombre de bases de E est $\gamma_{n,n}(q)$.

Un sous-espace vectoriel de dimension m de E est déterminé par une de ses bases. L'ensemble des sous-espaces vectoriels de dimension m de E s'identifie donc à l'ensemble quotient de l'ensemble des familles libres de m vecteurs de E par la relation d'équivalence $\sim$ définie par

$$(e_1, \ldots, e_m) \sim (e'_1, \ldots, e'_m) \Longleftrightarrow \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_m = \mathbb{K}e'_1 \oplus \cdots \oplus \mathbb{K}e'_m.$$

La classe de $(e_1, \ldots, e_m)$ est donc le nombre de bases de $\mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_m$, c'est-à-dire $\gamma_{m,m}(q)$. Le nombre de sous-espaces vectoriels de dimension m de E est donc $\dfrac{\gamma_{n,m}(q)}{\gamma_{m,m}(q)}$.

Exercice 30. *Soient $\mathbb{K}$ un corps fini, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$, m dans $\{0, \ldots, n\}$. Montrer que E a autant de sous-espaces vectoriels de dimension m que de sous-espace de dimension $n - m$.*

On démontre qu'un sous-espace vectoriel F d'un $\mathbb{K}$-espace de dimension finie E admet au moins un supplémentaire en prenant une base de E adaptée à F et en constatant que des vecteurs qui « complètent » une base de F en une base de E forment une base d'un supplémentaire de F dans E. Il est par ailleurs immédiat que tout supplémentaire de F dans E a pour dimension $\dim(E) - \dim(F)$.

Ici encore, des extensions à la dimension infinie sont possibles, mais nécessitent l'axiome du choix. Par exemple, on démontre qu'un sous-espace d'un espace vectoriel admet toujours un supplémentaire. Ces questions sont très marginales.

Exercice 31. *Soient E un $\mathbb{K}$-espace de dimension finie $n \geq 2$, F un sous-espace de E de dimension $m \in \{1, \ldots, n-1\}$. Montrer que F admet au moins deux supplémentaires dans E.*

Exercice 32. *Soient $\mathbb{K}$ un corps fini de cardinal q, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 2$, F un sous-espace de dimension m de E. Dénombrer les supplémentaires de F dans E.*

Exercice 33. *Soient n dans $\mathbb{N}^*$, k dans $\{0, \ldots, n\}$, C l'ensemble des vecteurs de $\mathbb{R}^n$ dont les coordonnées appartiennent à $\{0, 1\}$. Si V est un sous-espace de $\mathbb{R}^n$, on note $Z(V) = |V \cap C|$.*

a) Déterminer le minimum de $Z(V)$ lorsque V parcourt l'ensemble des sous-espaces de dimension k de $\mathbb{R}^n$.

b) Même question avec le maximum.

Exemple *Condition d'existence d'un supplémentaire commun*

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n, F et G deux sous-espaces de E. Il est clair que si F et G ont un supplémentaire commun, alors F et G ont même dimension.

Nous allons établir la réciproque en prouvant, si $m \in \{0, \ldots, n\}$, l'assertion $\mathcal{A}_m$: « si F et G sont deux sous-espaces de dimension m de E, alors F et G ont un supplémentaire commun ».

On raisonne par récurrence descendante sur m. Le cas $m = n$ est trivial. Supposons $m \leq n - 1$ et $\mathcal{A}_{m+1}$ démontrée. Soient F et G deux sous-espaces de dimension m de E. On sait que $F \cup G \neq E$. On choisit donc u dans $E \backslash (F \cup G)$. Les sommes $F + \mathbb{K}u$ et $G + \mathbb{K}u$ sont directes et les espaces $F \oplus \mathbb{K}u$ et $G \oplus \mathbb{K}u$ sont de dimension $m + 1$. Grâce à $\mathcal{A}_{m+1}$, ces sous-espaces admettent un supplémentaire commun S dans E. Mais alors, $S \oplus \mathbb{K}u$ est un supplémentaire commun à F et G dans E.

Le résultat suivant (« formule de Grassmann ») est simple et intuitif. On peut le voir comme la version linéaire du résultat ensembliste donnant le cardinal de la réunion de deux ensembles finis.

Théorème 5. *Soient E un $\mathbb{K}$-espace vectoriel, F et G deux sous-espaces de E de dimension finie. Alors $F + G$ est de dimension finie égale à*

$$dim(F) + dim(G) - dim(F \cap G).$$

Preuve abrégée 1. On part d'une base $(e_1, \ldots, e_r)$ de $F \cap G$, que l'on complète d'une part en une base $(e_1, \ldots, e_r, f_1, \ldots, f_p)$ de F, d'autre part en une base $(e_1, \ldots, e_r, g_1, \ldots, g_q)$ de G. Il est facile de voir que la famille de vecteurs $(e_1, \ldots, e_r, f_1, \ldots, f_p, g_1, \ldots, g_q)$ est une base de E, ce qui donne le résultat.

Preuve abrégée 2. L'espace $F \times G$ est naturellement paramétré (linéairement) par $F + G$. En effet, si, on pose, pour (x, y) dans $F \times G$:

$$\Phi(x, y) = x + y,$$

φ est une surjection linéaire de $F \times G$ sur $F + G$. Son noyau est

$$\{(x, -x),\ x \in F \cap G\},$$

naturellement isomorphe à $F \cap G$. La conclusion provient du théorème du rang.

Un corollaire immédiat est que si la dimension de E est strictement inférieure à $\dim(F) + \dim(G)$, alors $F \cap G$ n'est pas réduit à $\{0\}$.

L'exercice ci-après est une petite introduction à la théorie des codes correcteurs.

Exercice 34. *Soit n un élément de $\mathbb{N}^*$. On cherche à transmettre un message de n bits. Pour contrôler le message, on impose aux mots possibles d'appartenir à un sous-espace de ${\mathbb{F}_2}^n$. Un tel sous-espace est appelé code correcteur binaire linéaire. Soient C un tel code, non nul, k sa dimension.*

a) Vérifier qu'en posant, pour $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ dans ${\mathbb{F}_2}^n$,

$$\omega(x) = |\{i \in \{1, \ldots, n\},\ x_i \neq 0\}|, \qquad \delta(x, y) = \omega(x - y),$$

on obtient une distance sur $\mathbb{F}_2{}^n$ *(appelée « distance de Hamming »).*

b) On définit la distance minimale du code C *:*

$$d(C) = d = \min\{\omega(x),\ x \in C \setminus \{0\}\}.$$

Montrer que l'on peut corriger tout message comportant t *bits erronés si et seulement si* $2t \leq d-1$. *Ainsi,* d *quantifie la capacité de correction du code.*

c) Démontrer l'inégalité de Singleton : $d + k \leq n + 1$. *On pourra considérer l'intersection de* C *et du sous-espace de* $\mathbb{F}_2{}^n$ *constitué des vecteurs dont les* $n - d + 1$ *premières coordonnées sont nulles.*[11]

Rappelons également l'énoncé suivant.

Théorème 6. *Soient* $E_1, \ldots, E_m$ *des sous-espaces de dimension finie du* $\mathbb{K}$*-espace vectoriel* E. *Alors*

$$dim(E_1 + \cdots + E_m) \leq \sum_{i=1}^{m} dim(E_i).$$

Il y a égalité si et seulement si la somme $E_1 + \cdots + E_m$ *est directe.*

La preuve est immédiate à l'aide de l'application

$$(x_1, \ldots, x_m) \in E_1 \times \cdots \times E_m \longmapsto x_1 + \cdots + x_m.$$

5 Géométrie affine, convexité

5.1 Sous-espaces affines d'un espace vectoriel

Les espaces affines sont le cadre théorique de la *géométrie affine*, c'est-à-dire de la partie de la géométrie classique qui s'occupe des questions d'incidence et de parallélisme. Le programme se limite aux sous-espaces affines d'un espace vectoriel E. Les éléments de l'espace sont vus comme des points ou des vecteurs selon le cas. Un sous-espace affine est l'image d'un sous-espace vectoriel par une translation. Le sous-espace vectoriel en question est déterminé par le sous-espace affine qu'il dirige. Précisément, si V est un sous-espace vectoriel de E et a un élément de E, le sous-espace affine dirigé par V et passant par a est

$$A = V + a = \{a + v\ ;\ v \in V\}.$$

La relation

$$V = \left\{a' - a\ ;\ (a, a') \in A^2\right\}$$

montre que A détermine V : on dit que *V est la direction de A*, on note $V = \vec{A}$.[12] La dimension d'un sous-espace affine est celle de sa direction : un point est de dimension 0, une droite affine de dimension 1...

11. La borne de Singleton quantifie le fait que, pour une longueur n fixée, on ne peut pas avoir simultanément une capacité de correction importante et un grand nombre de mots.

12. En revanche, a n'est pas déterminé par A ; mieux $A = V + a'$ pour tout a' de A.

Remarques

1. *Intersection de sous-espaces affines*

   On vérifie qu'une intersection de sous-espaces affines de E est soit vide, soit un sous-espace affine de E dont la direction est l'intersection des directions des sous-espaces affines considérés. Cette constatation permet de définir le sous-espace affine de E engendré par une partie non vide X de E comme l'intersection des sous-espaces affines de E contenant X.

2. *Droite affine*

   Si a et b sont deux points distincts de E, *droite affine* passant par a et b est

   $$a + \mathbb{K}(b-a) = \{a + \lambda(b-a)\ ;\ \lambda \in \mathbb{K}\} = \{(1-\lambda)a + \lambda b\ ;\ \lambda \in \mathbb{K}\}.$$

   C'est le plus petit sous-espace affine de E contenant a et b.

3. *Équations linéaires non homogènes*

   La notion de sous-espaces affines apparaît dès que l'on considère une équation linéaire non homogène. Soient φ une application linéaire du $\mathbb{K}$-espace vectoriel E dans le $\mathbb{K}$-espace vectoriel F, a un élément de F. Alors l'ensemble des x de E tels que $\varphi(x) = a$ est soit vide[13], soit un sous-espace affine de E dirigé par $\mathrm{Ker}(\varphi)$.

   Exemples : les « systèmes linéaires »

   $$Ax = b, \quad A \in \mathcal{M}_{m,n}(\mathbb{K}), \quad b \in \mathcal{M}_{m,1}(\mathbb{K}),$$

   d'inconnue $x \in \mathcal{M}_{n,1}(\mathbb{K})$, mais aussi les équations linéaires avec second membre

   $$y' = a(x)y + b(x), \qquad y'' + ay' + by = c(x) \ldots$$

4. *Réunion d'un nombre fini de sous-espaces affines*

   Deux sous-groupes H et K d'un groupe G ont pour réunion un sous-groupe si seulement si l'un des deux contient l'autre. En effet, dans le cas contraire, on aurait $h \in H \setminus K$, $k \in K \setminus H$ et on voit que hk ne peut être dans $H \cup K$: s'il était dans H, $k = h^{-1}hk$ y serait également, le raisonnement est analogue dans l'autre cas.

   En particulier, la réunion de deux sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E n'est un sous-espace que si l'un d'entre eux contient l'autre. Nous allons donner une généralisation de ce résultat. Même si le cadre est général, l'intuition géométrique y est fondamentale. L'argument essentiel est en effet que l'intersection d'une droite affine D et d'un sous-espace affine est soit vide, soit réduite à un point, soit égale à D.

   Soit E un $\mathbb{K}$-espace vectoriel. Supposons que E soit réunion des sous-espaces affines stricts $V_1, \ldots, V_m$. Nous allons démontrer qu'alors $\mathbb{K}$ est fini de cardinal majoré par m.

   Quitte à supprimer certains V_i, ce qui diminue m, on peut supposer la réunion non redondante, c'est-à-dire qu'aucun des V_i n'est contenu dans la réunion des autres. Dans ce cas, on dispose de a dans $V_1 \setminus \cup_{i=2}^{m} V_i$ et

13. Tel est le cas si et seulement si a n'appartient pas à l'image de φ.

de b dans $V_2 \setminus V_1$. Ce choix de a et b assure que la droite affine D passant par a et b n'est contenue dans aucun des V_i. Elle coupe donc chaque V_i en au plus un point. Comme D est équipotente à $\mathbb{K}$, on obtient bien que $\mathbb{K}$ est fini de cardinal au plus m.

Exercice 35. *Déterminer le nombre de sous-espaces affines de dimension m d'un espace vectoriel de dimension n sur un corps $\mathbb{K}$ de cardinal q.*

Exercice 36. *Le corps $\mathbb{K}$ est infini, E est un $\mathbb{K}$-espace de dimension $n \in \mathbb{N}^*$. Une famille $(v_i)_{i\in I}$ de vecteurs de E est dite en position générale si, pour toute partie J de I de cardinal n, $(v_i)_{i\in J}$ est libre.*

a) Indiquer une famille $(v_i)_{i\in\mathbb{K}}$ de vecteurs de E en position générale. On pourra utiliser les matrices de Vandermonde.

b) En déduire que E n'est pas réunion finie de sous-espaces stricts.

Exercice 37. *On admet que tout espace vectoriel admet une base. Montrer que si E est un $\mathbb{K}$-espace de dimension infinie, E est réunion dénombrable d'hyperplans.*

Remarque *Définition intrinsèque des espaces affines*

L'assimilation points-vecteurs peut sembler un peu choquante. On peut en fait définir les espaces affines de manière intrinsèque. Soit E un $\mathbb{K}$-espace vectoriel. Une structure d'espace affine dirigé par E sur un ensemble $\mathcal{E}$ est une action simplement transitive du groupe $(E, +)$ sur $\mathcal{E}$, c'est-à-dire une application

$$(v, A) \in E \times \mathcal{E} \longmapsto A + v$$

telle que, pour tout couple (A, B) d'éléments de $\mathcal{E}$, il existe un unique v de E tel que $B = A+v$. On note alors $v = \overrightarrow{AB}$. À partir de cette définition, on reconstruit la géométrie affine et ses notions usuelles (sous-espaces affines, repères affines, barycentres). Le premier exemple est celui où $\mathcal{E} = E$ et où l'action est définie par l'addition des éléments de E. Cet exemple est en fait général : une fois fixée une origine sur $\mathcal{E}$, on peut « vectorialiser » cet espace affine. L'intérêt de la notion est donc principalement esthétique.

5.2 Barycentres

Une notion essentielle de géométrie affine est celle de *barycentre d'un système pondéré de points*. Soient $(a_1, \dots, a_m)$ des éléments de E, $(\lambda_1, \dots, \lambda_m)$ des éléments de $\mathbb{K}$ de somme non nulle. Alors, pour a dans E :

$$(1) \qquad \sum_{i=1}^{m} \lambda_i \, (a_i - a) = 0 \Longleftrightarrow a = \frac{\sum_{i=1}^{m} \lambda_i \, a_i}{\sum_{i=1}^{m} \lambda_i}.$$ [14]

Il existe donc exactement un point a vérifiant (1) : c'est le barycentre du système pondéré $(a_1, \dots, \lambda_1), \dots, (a_m, \lambda_m)$.

14. Dans le langage des espaces affines mentionné dans la remarque de **5.1**, la première relation s'écrit plus agréablement

$$\sum_{i=1}^{m} \lambda_i \; \overrightarrow{AA_i} = \vec{0}\,.$$

Remarques

1. *Homogénéité*

   Gardons les notations précédentes et considérons un élément μ de $\mathbb{K}^*$. Les systèmes pondérés $(a_1, \lambda_1), \dots, (a_m, \lambda_m)$ et $(a_1, \mu\lambda_1), \dots, (a_m, \mu\lambda_m)$ ont même barycentre.

2. *Milieu, isobarycentre*

   Si a et b sont deux points de E et si $\mathbb{K}$ n'est pas de caractéristique 2, le milieu de a et b est le barycentre de $(a, 1), (b, 1)$ ou encore $\dfrac{a+b}{2}$.

   Plus généralement, si $(a_1, \dots, a_m)$ sont des points de E et si la caractéristique de $\mathbb{K}$ ne divise pas m, on définit l'isobarycentre de $(a_1, \dots, a_m)$ comme le barycentre de $(a_1, 1), \dots, (a_m, 1)$.

3. *Caractérisation des espaces affines*

   Il est clair qu'un sous-espace affine de E est stable par barycentration. En fait, les parties de E stables par barycentration sont exactement les sous-espaces affines de E.

Exercice 38. *Démontrer cette dernière assertion. Donner une description en termes de barycentres du sous-espace affine de E engendré par une partie non vide X de E.*

Exemple *Médianes d'un triangle*

Supposons $\mathbb{K}$ de caractéristique différente de 2 et 3. Soient (a, b, c) trois points de E non situés sur une même droite affine. Les médianes du triangle de sommets a, b, c sont, par définition, les droites joignant a au milieu de (b, c) etc... L'isobarycentre de a, b, c est le barycentre de $(a, \frac{1}{3}), (\frac{a+b}{2}, \frac{2}{3})$. Il appartient donc à la médiane issue de a. Les rôles des points a, b, c étant symétriques, l'isobarycentre de (a, b, c) appartient à toute médiane.

5.3 Convexité

Généralités

Si $\mathbb{K} = \mathbb{R}$, on peut définir plusieurs notions géométriques liés à la relation d'ordre usuelle. La plus importante est la notion de *partie convexe*. Soit, dans **5.2**, E un $\mathbb{R}$-espace vectoriel. Si a et b sont deux points de E, on note $[a, b]$ le segment :

$$[a, b] = \{(1-t)a + tb),\ t \in [0, 1]\}.$$

Une partie X de E est dite convexe si

$$\forall (a, b) \in X^2, \qquad [a, b] \subset X.$$

Une intersection quelconque de convexes est convexe. On en déduit, si X est une partie de E, que l'intersection des convexes de E contenant X est convexe. C'est donc le plus petit convexe de E contenant X, on l'appelle *enveloppe convexe de* X et on le note $\mathrm{Conv}(X)$. On établit aisément le résultat suivant.

Lemme 1. *L'enveloppe convexe de X est*

$$\left\{ \sum_{i=1}^{p} \lambda_i x_i \ ; \ p \in \mathbb{N}^*, \ (x_1, \ldots, x_p) \in X^p, \ (\lambda_1, \ldots, \lambda_p) \in \mathbb{R}^{+p}, \ \sum_{i=1}^{p} \lambda_i = 1 \right\}.$$

Traduction en terme de barycentres : une partie de E est convexe si et seulement si elle est stable par barycentration positive ; l'enveloppe convexe de X est l'ensemble des barycentres à coefficients positifs d'éléments de X.

Exemples

1. Les sous-espaces affines d'un espace vectoriel réel sont convexes.
2. Soient φ une forme linéaire continue sur E, non identiquement nulle, a dans $\mathbb{R}$. Alors $\varphi^{-1}([a, +\infty[)$ est une partie convexe de E ; les convexes de ce type sont appelés « demi-espaces fermés » de E.
3. Soient a, b, c trois points de E. L'enveloppe convexe de $\{a, b\}$ est le segment $[a, b]$, celle de $\{a, b, c\}$ est le triangle plein de sommets a, b, c.
4. Plus généralement, l'enveloppe convexe d'un ensemble fini est ce que l'on appelle un *polyèdre* compact.[15] L'enveloppe convexe de $n1+$ points affinement indépendants est appelée un $n + 1$-*simplexe*.
5. L'enveloppe convexe de la sphère unité d'un espace vectoriel normé est la boule unité fermée.
6. Soit P dans $\mathbb{C}[X]$ non constant. Dans le plan complexe vu comme espace réel de dimension 2), l'enveloppe convexe des zéros de P contient tous les zéros de P' (théorème de Gauss-Lucas, démontré dans le cours sur les polynômes).
7. Nous verrons dans le cours sur les espaces euclidiens que tout convexe fermé d'un espace normé réel de dimension finie est intersection de demi-espaces fermés.[16]

Exercice 39. *Démontrer l'assertion de l'exemple 2.*

Le théorème de Carathéodory

Pour préciser le lemme en dimension finie et donner une illustration non triviale de la convexité, nous allons établir le résultat géométrique suivant, connu comme *théorème de Carathéodory*.

Théorème 7. *Soient E un $\mathbb{R}$-espace de dimension n, X une partie de E. Tout point de l'enveloppe convexe de X s'écrit*

$$\sum_{i=1}^{n+1} \lambda_i x_i$$

où les x_i sont des éléments de X, les λ_i des éléments de $\mathbb{R}^+$ de somme 1.[17]

15. Si E est de dimension finie, on démontre que les polyèdres compacts de E sont exactement les parties compactes de E qui sont intersection finie de demi-espaces. Ce résultat, qui peut sembler intuitivement assez clair, demande en fait un certain travail.

16. Résultat également vraie en dimension infinie, mais la démonstration devient un peu plus compliquée.

17. Le nombre $n + 1$ de l'énoncé est clairement optimal.

Preuve. Nous utiliserons le lemme suivant.

Lemme 2. *Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n, $(v_i)_{1 \leq i \leq m}$ une famille d'éléments de E avec $m \geq n+2$. Alors il existe $(\lambda_1, \ldots, \lambda_m)$ non nul dans $\mathbb{K}^m$ tel que :*

$$\sum_{i=1}^{m} \lambda_i v_i = 0, \qquad \sum_{i=1}^{m} \lambda_i = 0.$$

Preuve. L'application

$$\varphi \ : (\lambda_1, \ldots, \lambda_m) \in \mathbb{K}^m \longmapsto \left(\sum_{i=1}^{m} \lambda_i v_i, \sum_{i=1}^{m} \lambda_i \right) \in E \times \mathbb{K}$$

est manifestement linéaire. L'espace source est de dimension m, l'espace but de dimension $n+1 < m$. Il s'ensuit que φ ne peut être injective.

Retour au théorème de Carathéodory. Soit x un point de l'enveloppe convexe de X. On dispose donc de m dans $\mathbb{N}^*$, de m points $x_1, \ldots, x_m$ de X et de m éléments de $\mathbb{R}^+$ de somme 1, $\lambda_1, \ldots, \lambda_m$ tels que

$$x = \sum_{i=1}^{m} \lambda_i x_i.$$

Si $m \leq n+1$, on a gagné. Supposons $m \geq n+2$. Nous allons montrer que x peut s'écrire comme barycentre positif de $m-1$ des x_i. Le résultat s'en déduira immédiatement par récurrence finie. Le lemme précédent nous donne $(\mu_1, \ldots \mu_m)$ dans $\mathbb{R}^m \setminus \{0\}$ tel que

$$\sum_{i=1}^{m} \mu_i x_i = 0, \qquad \sum_{i=1}^{m} \mu_i = 0.$$

On a donc, si α est un réel :

$$x = \sum \left(\lambda_i + \alpha \mu_i \right) x_i.$$

Les $\lambda_i + \alpha\mu_i$ ont pour somme 1. Nous allons montrer que l'on peut choisir α de sorte qu'ils soient tous dans $\mathbb{R}^+$ et que l'un au moins d'entre eux soit nul, ce qui achèvera la démonstration. Puisque les μ_i sont non tous nuls et ont pour somme 0, les ensembles

$$I^+ = \{ i \in \{1, \ldots, m\}, \ \mu_i > 0 \}, \qquad I^- = \{ i \in \{1, \ldots, m\}, \ \mu_i < 0 \}$$

sont non vides. La positivité des $\lambda_i + \alpha\mu_i$ s'écrit

$$\forall i \in I^+, \ \alpha \geq -\frac{\lambda_i}{\mu_i}, \quad \forall i \in I^-, \ \alpha \leq -\frac{\lambda_i}{\mu_i}.$$

Prenons donc

$$\alpha = \max \left\{ -\frac{\lambda_i}{\mu_i}, \ i \in I^+ \right\}.$$

Par choix de α, les $\lambda_i + \alpha\mu_i$ pour i dans I^+ sont dans $\mathbb{R}^+$ et l'un d'entre eux est nul. Comme α est dans $\mathbb{R}^-$, les $\lambda_i + \alpha\mu_i$ pour i dans I^- sont dans $\mathbb{R}^+$. Le résultat est établi.

Exercice 40. *Déduire du théorème de Carathéodory que, si X est une partie compacte d'une espace réel de dimension finie, l'enveloppe convexe de X est compacte.*

Exercice 41. *Soient E un $\mathbb{R}$-espace vectoriel de dimension n, $x_1, \dots, x_{n+2}$ des points de E. Montrer qu'il existe une partition de $\{1, \dots, n+2\}$ en deux ensembles I et J tels que l'enveloppe convexe de $\{x_i,\ i \in I\}$ coupe celle $\{x_i,\ i \in J\}$* [18].

Points extrémaux

Soit C un convexe de E. Un point a de C est *extrémal* si

$$\forall (x, y) \in C^2, \qquad a = \frac{x+y}{2} \Longrightarrow x = y = a.$$

Exemples

1. Les points extrémaux d'un segments sont ses extrémités, les points extrémaux d'un triangle sont ses sommets.
2. Les points extrémaux de la boule unité fermée d'un espace préhilbertien réel sont ceux de la sphère unité.
3. Une droite, une boule ouverte d'un espace euclidien, n'ont pas de points extrémaux.
4. Les exemples précédents suggèrent qu'une hypothèse de compacité s'impose si l'on souhaite reconstruire un convexe à partir de ses points extrémaux. De fait, on démontre qu'un convexe compact d'un espace réel de dimension finie est enveloppe convexe de ses points extrémaux (théorème de Minkovski), qu'un convexe compact d'un espace normé réel est l'adhérence de l'enveloppe convexe de ses points extrémaux (théorème de Krein-Milman).

Exercice 42. *Soit E l'espace des fonctions continues de $[0,1]$ dans $\mathbb{R}$. Déterminer les points extrémaux de la boule unité fermée de E pour chacune des normes $\| \ \|_2$, $\| \ \|_\infty$ et $\| \ \|_1$.*

Exercice 43. *Montrer qu'un convexe compact non vide C d'un espace normé réel E de dimension finie possède au moins un point extrémal. On pourra considérer une norme euclidienne sur E et maximiser cette norme sur C.*

Exercice 44. *On suppose E de dimension n. Soient $\varphi_1, \dots, \varphi_m$ des formes linéaires sur E, $\alpha_1, \dots, \alpha_m$ des nombres réels,*

$$P = \bigcap_{i=1}^{m} \{x \in E \ ; \ \varphi(x) \leq \alpha_i\}.$$

Si $x \in P$, soit $I(x) = \{i \in \{1, \dots, m\} \ ; \ \varphi_i(x) = \alpha_i\}$.

a) Montrer qu'un point x de P est un point extrémal de P si et seulement si

$$\mathit{Vect}\{\varphi_i,\ i \in I(x)\} = E^*.$$

b) Soit x un point extrémal de P. Montrer : $|I(x)| \geq n$.

c) On suppose que l'ensemble des poins extrémaux de P est non vide. Montrer que $m \geq n$ et que le cardinal des points extrémaux de P est majoré par $\binom{m}{n}$

18. Résultat dû à Radon.

Exercice 45. *Soit $n \in \mathbb{N}^*$. Montrer que les points extrémaux de l'ensemble des matrices bistochastiques de $\mathcal{M}_n(\mathbb{R})$ sont les matrices de permutation.*