Chapitre 29

Applications linéaires

Comme d'habitude, conformément au programme, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$, mais la plupart des résultats restent valables sur un corps $\mathbb{K}$ quelconque. De plus, E, F et G désignent des $\mathbb{K}$-espaces vectoriels.

Plus précisément, tous les résultats du chapitre restent valables sur un corps quelconque, sauf ceux du paragraphe V.2.

I Applications linéaires

I.1 Définition, caractérisation pratique

Définition. Soit $u : E \to F$. On dit que u est une application linéaire (AL) si :

$$\forall (x,y) \in E^2, \forall \lambda \in \mathbb{K}, \qquad u(x+y) = u(x) + u(y) \qquad \text{et} \qquad u(\lambda x) = \lambda u(x)$$

Remarques :

- La définition est en fait assez naturelle étant donnée la définition d'un espace vectoriel : une application est linéaire quand elle est compatible avec les lois externe et interne qui définissent un espace vectoriel. De façon plus générale, dès qu'on définit une structure, il est naturel de définir des applications compatibles avec les lois de cette structure. Cette définition est à rapprocher de la définition d'un morphisme de groupes et d'un morphismes d'anneaux : une fois ceci compris, la définition d'une application linéaire est totalement naturelle.
- D'ailleurs, la première propriété d'une application d'une AL (« elle casse la somme ») fait qu'une AL est en particulier un morphisme de groupes entre les groupes abéliens $(E,+)$ et $(F,+)$. En particulier, une AL envoie le neutre sur le neutre, c'est-à-dire :

Proposition (Condition NÉCESSAIRE importante). Soit u linéaire. Alors $u(0_E) = 0_F$.

Remarque : La réciproque est fausse ! Voir plus bas pour des exemples. Là aussi, cette condition est surtout importante pour sa contraposée :

Corollaire. Soit $u : E \to F$. Si $u(0_E) \neq 0_F$, alors u n'est pas linéaire.

Proposition (Caractérisation pratique bis). Soit $u : E \to F$. u est une AL si et seulement si :

$$\forall (x,y) \in E^2, \forall (\lambda, \mu) \in \mathbb{K}^2, u(\lambda x + \mu y) = \lambda u(x) + \mu u(y)$$

Démonstration. Supposons que u soit linéaire. Soit $(x,y) \in E^2$ et soit $(\lambda,\mu) \in \mathbb{K}^2$. En utilisant les deux propriétés d'une AL, on obtient successivement :

$$\begin{aligned} u(\lambda x + \mu y) &= u(\lambda x) + u(\mu y) \\ &= \lambda u(x) + \mu u(y) \end{aligned}$$

Réciproquement, supposons que pour tous $(x,y) \in E^2$ et $(\lambda,\mu) \in \mathbb{K}^2$, $u(\lambda x + \mu y) = \lambda x + \mu y$, et montrons que u est linéaire. Soit $(x,y) \in E^2$ et soit $\lambda \in \mathbb{K}$. Tout d'abord :

$$\begin{aligned} u(x+y) &= u(1.x + 1.y) \\ &= 1.u(x) + 1.u(y) \\ &= u(x) + u(y) \end{aligned}$$

et on a également

$$\begin{aligned} u(\lambda x) &= u(\lambda x + 0.y) \\ &= \lambda u(x) + 0.u(y) \\ &= \lambda u(x) \end{aligned}$$ □

si bien que u est linéaire.

Remarques :

- En particulier, sur le plan vectoriel $\text{Vect}(x, y)$, u est entièrement déterminée par $u(x)$ et $u(y)$. Il suffit donc de connaître l'image de ces deux vecteurs pour connaître l'image de tous les vecteurs du plan qu'ils engendrent. Nous généraliserons cette idée dans le paragraphe IV.
- Comme pour prouver qu'une partie de E est un sev de E, nous utiliserons indifféremment la définition ou la caractérisation pratique bis pour prouver qu'une application est linéaire.
- Comme dans le chapitre 28, il existe un critère mixte (dont la démonstration est laissée en exo) que nous n'utiliserons jamais : une application $u : E \to F$ est linéaire si et seulement si :

$$\forall (x, y) \in E^2, \forall \lambda \in \mathbb{K}, u(\lambda x + y) = \lambda u(x) + u(y)$$

Mais que vous rencontrerez souvent quand vous évoluerez dans un univers (hostile) extérieur à ma classe.

Corollaire (Linéarité généralisée). Soit $u : E \to F$ linéaire. Alors, pour toute famille $(x_i)_{i\in I}$ d'éléments de E et toute famille presque nulle de scalaires $(\lambda_i)_{i\in I}$,

$$u\left(\sum_{i\in I} \lambda_i x_i\right) = \sum_{i\in I} \lambda_i u(x_i)$$

Démonstration. On prouve par récurrence, à l'aide de la proposition précédente, le résultat suivant :

$$\forall n \geqslant 1, \forall (x_1, \ldots, x_n) \in E^n, \forall (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n, u\left(\sum_{k=1}^{n} \lambda_k x_k\right) = \sum_{k=1}^{n} \lambda_k u(x_k)$$ □

ce qui permet de conclure, une famille presque nulle étant une famille n'ayant qu'un nombre fini de termes non nuls.

Remarques :

- Une application linéaire est donc compatible avec toutes les opérations qu'on peut effectuer dans un espace vectoriel (j'ai envie de dire : c'est fait pour).
- De même, si u est linéaire, il suffit donc de connaître l'image de $x_1, \ldots, x_n$ pour connaître l'image de tout élément de $\text{Vect}(x_1, \ldots, x_n)$. On généralisera cette notion dans le IV.

I.2 Cas particuliers : endomorphismes, isomorphismes, automorphismes

Définition. Soit $u : E \to F$ linéaire.

- Si $E = F$, u est un endomorphismes de E.
- Si u est bijective, u est un isomorphisme.
- Si u est à la fois un isomorphisme et un endomorphisme, u est un automorphisme de E.

Remarque : En d'autres termes, un endomorphisme est une application linéaire d'un espace dans lui-même, et un automorphisme est une application linéaire bijective d'un espace dans lui-même.

Définition. S'il existe un isomorphisme $u : E \to F$, alors E et F sont dits isomorphes.

Comme pour les groupes : deux espaces vectoriels sont isomorphes lorsque ce sont « les mêmes », lorsqu'ils représentent le même modèle d'espace vectoriel. Voir des exemples dans la suite.

I.3 Exemples

- Les applications linéaires de $\mathbb{K}$ dans $\mathbb{K}$ (donc les endomorphismes de $\mathbb{K}$) sont exactement les fonctions de la forme

$$\left\{\begin{array}{ccc}\mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & ax\end{array}\right.$$

où a est un élément de $\mathbb{K}$ quelconque. Soit en effet $u : \mathbb{K} \to \mathbb{K}$ linéaire. Soit $\lambda \in \mathbb{K}$. Alors

$$\begin{aligned} u(\lambda) &= u(\lambda.1) \\ &= \lambda u(1) \end{aligned}$$

En posant $a = u(1)$, il vient $u(\lambda) = a\lambda$, donc u est bien de la forme demandée. Réciproquement, soit $a \in \mathbb{R}$ et soit

$$u : \left\{\begin{array}{ccc}\mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & ax\end{array}\right.$$

Montrons que u est linéaire. Soient $(x, y) \in \mathbb{K}^2$ et $\lambda \in \mathbb{K}$.

$$\begin{aligned} u(x+y) &= a \times (x+y) \\ &= ax + ay \\ &= u(x) + u(y) \end{aligned}$$

et

$$\begin{aligned} u(\lambda x) &= a \times \lambda x \\ &= \lambda \times ax \\ &= \lambda u(x) \end{aligned}$$

u est bien linéaire.

- Exemple type classique : soit

$$u : \left\{\begin{array}{ccc}\mathbb{K}^3 & \to & \mathbb{K}^2 \\ (x_1, x_2, x_3) & \mapsto & (x_1 + x_2 - x_3, 2x_1 - 4x_3)\end{array}\right.$$

Comme dans le chapitre 28, il faut lire : « (première coordonnée + deuxième coordonnée − troisième coordonnée, 2×(première coordonnée) − 4×(troisième coordonnée)) ».

Montrons que u est linéaire. Soient $x = (x_1, x_2, x_3)$ et $y = (y_1, y_2, y_3)$ appartenant à $\mathbb{K}^3$ et $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, \lambda x_3 + \mu y_3)$$

donc

$$\begin{aligned}u(\lambda x+\mu y) &= (\lambda x_1+\mu y_1+\lambda x_2+\mu y_2-\lambda x_3-\mu y_3, 2(\lambda x_1+\mu y_1)-4(\lambda x_3+\mu y_3))\\ &= (\lambda(x_1+x_2-x_3)+\mu(y_1+y_2-y_3), \lambda(2x_1-4x_3)+\mu(2y_1-4y_3))\\ &= \lambda(x_1+x_2-x_3, 2x_1-4x_3)+\mu(y_1+y_2-y_3, 2y_1-4y_3)\\ &= \lambda u(x)+\mu u(y)\end{aligned}$$

u est linéaire. Plus généralement, entre $\mathbb{K}^n$ et $\mathbb{K}^p$, toute application qui renvoie des combinaisons linéaires de coordonnées de x est linéaire, il faut savoir les repérer au premier coup d'oeil. Par exemple,

$$u : \begin{cases} \mathbb{K}^n & \to & \mathbb{K} \\ (x_1, \dots, x_n) & \mapsto & x_1 + 4x_2 + \cdots + n^2 x_n = \displaystyle\sum_{k=1}^n k^2 x_k \end{cases}$$

Mais, comme dans le chapitre 28, il faut être prudent : par exemple, il n'est pas évident que $(x,y) \mapsto (x+1)^2 - x^2 - (3y+1)$ est linéaire ! De plus, contrairement au chapitre 28, on ne dispose pas d'un résultat général permettant de l'affirmer directement (même si on le fera souvent en pratique).

est linéaire : en effet, soient $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ deux éléments de $\mathbb{K}^n$, et $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1, \dots, \lambda x_2 + \mu y_2)$$

si bien que

$$\begin{aligned}u(\lambda x+\mu y) &= \sum_{k=1}^n k^2(\lambda x_k + \mu y_k)\\ &= \lambda \sum_{k=1}^n k^2 x_k + \mu \sum_{k=1}^n k^2 y_k\\ &= \lambda u(x) + \mu u(y)\end{aligned}$$

On aurait pu simplement dire « par linéarité de la somme », comme on dira plus tard « par linéarité de l'intégrale », mais il faut être prudent avec ces formulation et ne pas l'employer n'importe quand. Par exemple,

$$u : \begin{cases} \mathbb{K}^n & \to & \mathbb{K} \\ (x_1, \dots, x_n) & \mapsto & {x_1}^2 + {x_2}^2 + \cdots + {x_n}^2 = \displaystyle\sum_{k=1}^n {x_k}^2 \end{cases}$$

ne l'est pas (alors que $u(0, \dots, 0) = 0$). En effet, $u(1, \dots, 1) = n$ mais $u(2, \dots, 2) = 4n \neq 2u(1, \dots, 1)$.

Pour prouver qu'une fonction n'est pas linéaire, il faut un contre-exemple EXPLICITE !

- L'application

$$u : \begin{cases} \mathbb{R}^{\mathbb{R}} & \to & \mathbb{R} \\ f & \mapsto & f(2024) \end{cases}$$

est linéaire. En effet, si f et g appartiennent à $\mathbb{R}^{\mathbb{R}}$ et $(\lambda, \mu) \in \mathbb{K}^2$,

$$\begin{aligned}u(\lambda f+\mu g) &= (\lambda f + \mu g)(2024)\\ &= \lambda f(2024) + \mu g(2024)\\ &= \lambda u(f) + \mu u(g)\end{aligned}$$

Cette application est appelée évaluation en 2024 : on parlera donc parfois de la linéarité de l'évaluation.

- L'application

$$u : \begin{cases} D(\mathbb{R},\mathbb{R}) & \to & \mathbb{R} \\ \\ f & \mapsto & f'(2024) \end{cases}$$

est linéaire. On peut le dire directement car on a vu que la dérivation est linéaire (cf chapitre sur la dérivation), mais on le montrerait de même que ci-dessus.

- L'application

$$u : \begin{cases} \mathscr{C}^\infty(\mathbb{R},\mathbb{R}) & \to & \mathscr{C}^\infty(\mathbb{R},\mathbb{R}) \\ \\ f & \mapsto & f' \end{cases}$$

est un endomorphisme (u est linéaire par linéarité de la dérivation, et est bien à valeurs dans $\mathscr{C}^\infty(\mathbb{R},\mathbb{R})$ car la dérivée d'une fonction $\mathscr{C}^\infty$ est $\mathscr{C}^\infty$) mais pas un automorphisme car n'est pas injectif (en effet, si f et g sont respectivement la fonction nulle et la fonction constante égale à 1 alors $u(f) = u(g) = 0$, la fonction nulle).

- L'application

$$u : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ \\ (x,y) & \mapsto & (y,x) \end{cases}$$

est un automorphisme car est linéaire (exo) et bijective (c'est une involution).

- L'application

$$u : \begin{cases} \mathbb{K}^2 & \to & \mathbb{K}_1[X] \\ \\ (a,b) & \mapsto & aX+b \end{cases}$$

est un isomorphisme car est linéaire et bijective (exo). On en déduit que $\mathbb{R}^2$ et $\mathbb{R}_1[X]$ sont isomorphes.

On le reprouvera avec des arguments de dimension dans le chapitre 30. Puisqu'un polynôme de degré inférieur ou égal à 1 est entièrement déterminé par le coefficient constant et le coefficient devant X, cet isomorphisme n'est pas très étonnant (les deux espaces vectoriels sont « les mêmes »). De même, pour tout n, $\mathbb{K}_n[X]$ et $\mathbb{K}^{n+1}$ sont isomorphes (on le prouvera aussi dans le chapitre 30).

- L'application

$$u : \begin{cases} D(\mathbb{R},\mathbb{R}) & \to & \mathbb{R}^\mathbb{R} \\ \\ f & \mapsto & f' \end{cases}$$

est linéaire.

Remarque : la dérivation est une bonne illustration de l'avant-dernière remarque du paragraphe précédent, c'est-à-dire que connaître l'image des vecteurs $x_1, \dots, x_n$ suffit pour connaître l'image de tout élément de $\text{Vect}(x_1, \dots, x_n)$. En effet, par exemple, connaître la dérivée des fonctions $\left(x \mapsto x^k\right)_{k \in [\![0\,;\,n]\!]}$ suffit pour connaître la dérivée de toute fonction polynomiale de degré inférieur ou égal à n. Encore une fois, on généralisera tout cela dans le 4.

- L'application

$$u : \begin{cases} \mathscr{C}(\mathbb{R},\mathbb{R}) & \to & \mathbb{R} \\ \\ f & \mapsto & \displaystyle\int_{2023}^{2024} f(t)dt \end{cases}$$

est linéaire, par linéarité de l'intégrale.

- L'application

$$u : \left\{ \begin{array}{ccc} \mathscr{M}_{n,p}(\mathbb{K}) & \to & \mathscr{M}_{p,n}(\mathbb{K}) \\ & & \\ M & \mapsto & M^\top \end{array} \right.$$

est linéaire, par linéarité de la transposition. C'est même un isomorphisme car la transposition est une bijection (cf. chapitre 21) mais ce n'est un automorphisme que si $n = p$ i.e. les matrices sont carrées.

- Soit $(\Omega, \mathscr{P}(\Omega), P)$ est un espace probabilisé fini. L'espérance

$$E : \left\{ \begin{array}{ccc} \mathbb{K}^\Omega & \to & \mathbb{K} \\ & & \\ X & \mapsto & E(X) \end{array} \right.$$

est linéaire par linéarité de l'espérance (E désigne évidemment ici l'opérateur espérance, pas un espace vectoriel, et X une variable aléatoire).

On sait (cf. chapitre 28) que si E est un espace vectoriel et si X est un ensemble quelconque, alors E^X est muni d'une structure d'espace vectoriel. En particulier, $\mathbb{K}^\Omega$ est un $\mathbb{K}$-espace vectoriel.

- L'application

$$\mathrm{Id}_E : \left\{ \begin{array}{ccc} E & \to & E \\ & & \\ x & \mapsto & x \end{array} \right.$$

est linéaire et, plus généralement, pour tout $\alpha \in \mathbb{K}$, $\alpha \mathrm{Id}_E$ est linéaire. Les AL de la forme $\alpha \mathrm{Id}_E$ sont appelées homothéties. Celles-ci peuvent être caractérisées de façon très simple :

Activité : Soit $u \in \mathscr{L}(E)$. Montrons que si, pour tout $x \in E$, x et $u(x)$ forment une famille liée, alors u est une homothétie.

Très classique ! Cette question peut être posée à l'écrit sans autre forme de procès !

Par hypothèse, pour tout x, x et $u(x)$ sont colinéaires : soit il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$, soit il existe μ tel que $x = \mu u(x)$, mais si $\mu \neq 0$ alors $u(x) = (1/\mu).x$, et si $\mu = 0$, alors $x = 0$ donc $u(x) = 0 = x$. Dans tous les cas, on vient de prouver qu'il existe $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$, et le but est de prouver que u est une homothétie, donc qu'il existe $\lambda \in \mathbb{K}$ tel que, pour tout $x \in E$, $u(x) = \lambda x$. La différence entre l'hypothèse et ce qu'on veut prouver est que le λ de l'hypothèse n'est a priori pas le même pour tout vecteur x, alors qu'on veut montrer qu'il existe un même scalaire λ qui convient pour tout le monde.

Explicitons la dépendance de λ par rapport à x : par hypothèse, pour tout x, il existe $\lambda_x \in \mathbb{K}$ tel que $u(x) = \lambda_x.x$. Soient x et y deux éléments de E : prouvons que $\lambda_x = \lambda_y$.

Premier cas : x et y sont libres. Par linéarité de u,

$$\begin{array}{rcl} u(x+y) & = & u(x) + u(y) \\ & = & \lambda_x.x + \lambda_y.y \end{array}$$

Or, par hypothèse, il existe également λ_{x+y} tel que

$$\begin{array}{rcl} u(x+y) & = & \lambda_{x+y}.(x+y) \\ & & \\ & = & \lambda_{x+y}.x + \lambda_{x+y}.y \end{array}$$

Par unicité des coefficients d'une famille libre, $\lambda_x = \lambda_{x+y}$ et $\lambda_y = \lambda_{x+y}$ et, en particulier, $\lambda_x = \lambda_y$.

Deuxième cas : x et y sont liés et non nuls. Il existe $\alpha \in \mathbb{K}$ non nul tel que $x = \alpha y$. D'une part, $u(x) = \lambda_x.x = \lambda_x \alpha.y$ et d'autre part, par linéarité de u,

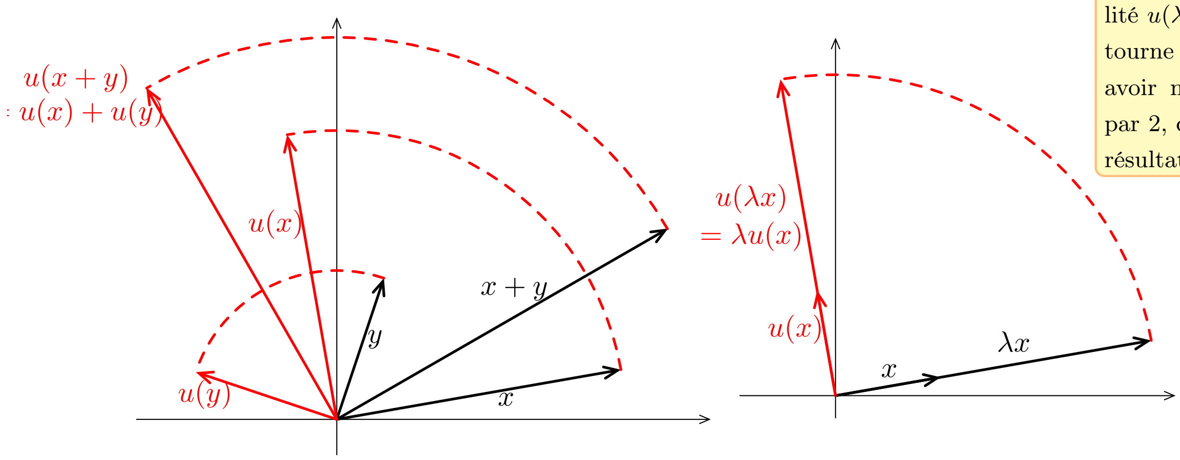
$$\begin{array}{rcl} u(x) & = & u(\alpha y) \\ & = & \alpha u(y) \\ & = & \alpha \lambda_y.y \end{array}$$

si bien que $\alpha.\lambda_x = \alpha.\lambda_y$ et α est non nul donc $\lambda_x = \lambda_y$. Finalement, que x et y soient libres ou liés non nuls, $\lambda_x = \lambda_y$: il existe donc $\lambda \in \mathbb{K}$ tel que, pour tout $x \in E$ non nul, $u(x) = \lambda x$, et cette égalité est encore valable pour $x = 0_E$: $u = \lambda \operatorname{Id}_E$.

Donnons à présent des exemples plus « géométriques » :

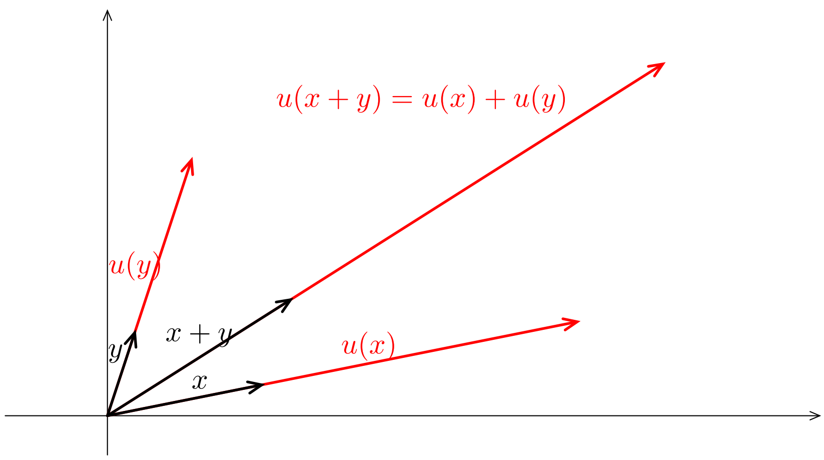
- Rotations :

Par exemple, pour l'égalité $u(\lambda x) = \lambda u(x)$: qu'on tourne avant ou après avoir multiplié le vecteur par 2, cela donne le même résultat.



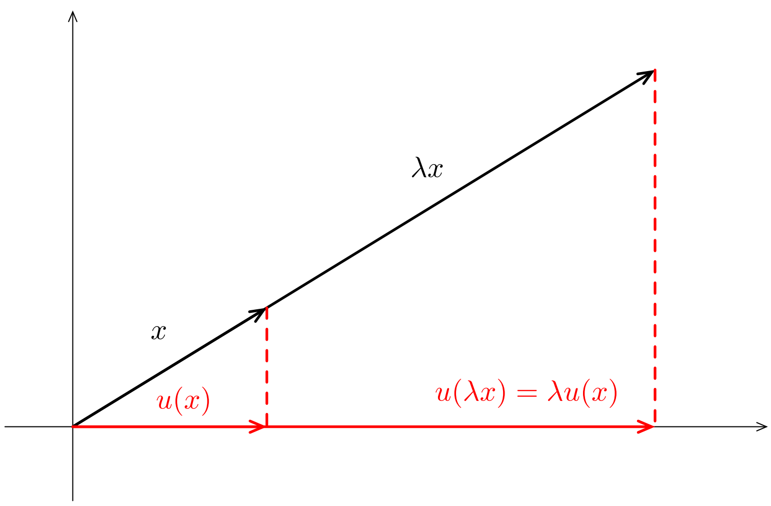
- Homothéties :

On ne fait un dessin que pour illustrer l'égalité $u(x+y) = u(x) + u(y)$ et pas l'égalité $u(\lambda x) = \lambda u(x)$, mais on ferait pour celle-ci un dessin tout-à-fait analogue.



- Projections orthogonales (attention, il existe des projections non orthogonales, cf III) :

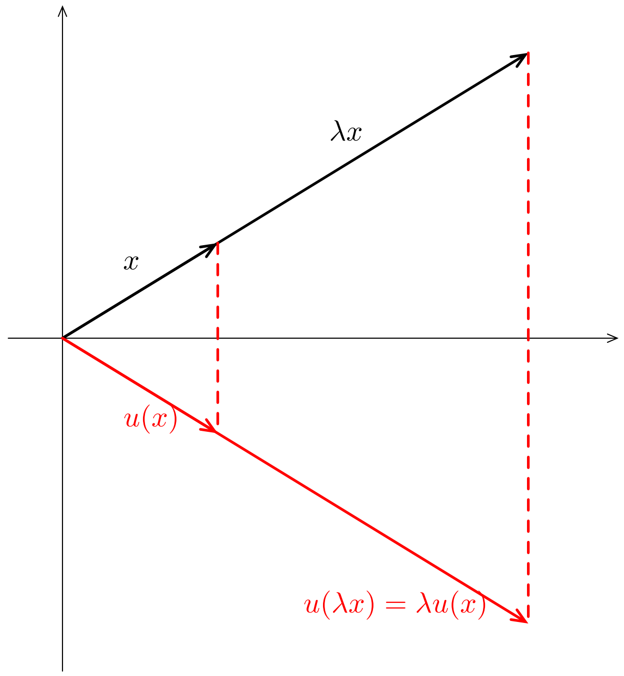
On peut voir une projection comme une ombre (et une projection orthogonale comme l'ombre obtenue lorsque le soleil est au zénith). Par exemple, qu'on multiplie le vecteur par 2 avant ou après la projection, cela donnera le même résultat. Par exemple, si vous doublez la longueur d'un bâton, l'ombre sera deux fois plus longue !



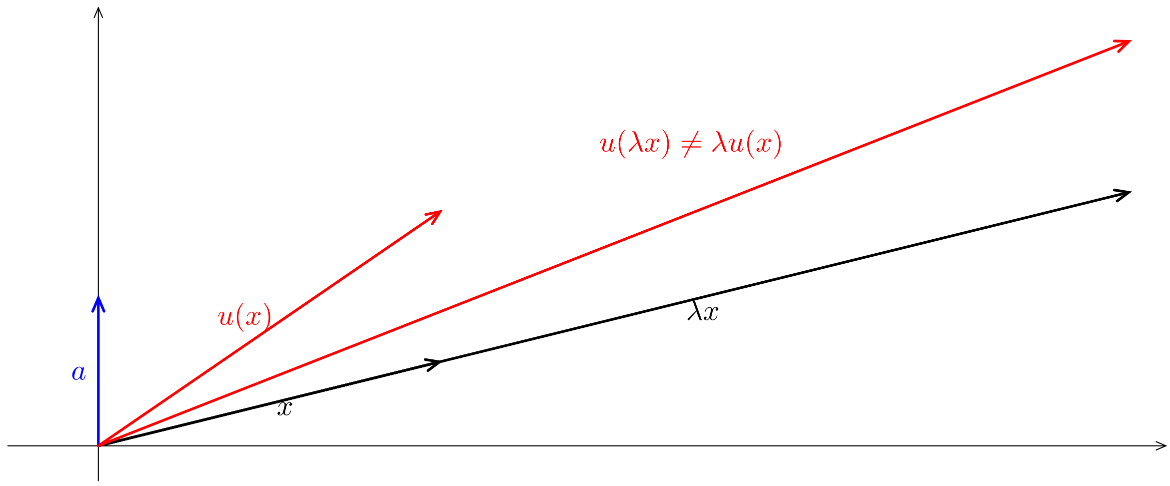
Idem, on ne fait pas le dessin représentant l'égalité $u(x+y) = u(x)+u(y)$ par flemme.

Là aussi, il existe des symétries non orthogonales, cf. paragraphe V.2.

- Symétries orthogonales :



- Cependant, une translation n'est pas une application linéaire (sauf une translation de vecteur nul...) car l'image du vecteur nul n'est pas le vecteur nul, et on sait que c'est une condition nécessaire. Ci-dessous, on a représenté la translation de vecteur a (c'est-à-dire l'application $u : x \mapsto x + a$) :



Donnons un dernier exemple pour la route : un exemple dans un espace de fonctions. Soit

$$u : \left\{ \begin{array}{ccc} \mathscr{C}(\mathbb{R}, \mathbb{R}) & \to & \mathbb{R}^{\mathbb{R}} \\ f & \mapsto & \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\int_x^{x+1} f(t)dt \end{array} \right. \end{array} \right.$$

Montrer que u est linéaire.

Soient $(f,g)\in\mathscr{C}(\mathbb{R},\mathbb{R})^2, (\lambda,\mu)\in\mathbb{R}^2$. Soit $x\in\mathbb{R}$ (à ne pas oublier, ni ici ni dans les lignes suivantes !).

Attention à la rédaction, comme dans le chapitre 28 lorsqu'on montrait des résultats de liberté pour des familles de fonctions.

$$\begin{aligned} u(\lambda f+\mu g)(x) &= \int_x^{x+1} \lambda f(t)+\mu g(t)dt \\ &= \lambda\int_x^{x+1} f(t)dt+\mu\int_x^{x+1} g(t)dt \qquad \text{(linéarité de l'intégrale)} \\ &= \lambda u(f)(x)+\mu u(g)(x) \\ &= (\lambda u(f)+\mu u(g))(x) \end{aligned}$$

Ainsi, les fonctions $u(\lambda f+\mu g)$ et $\lambda u(f)+\mu u(g)$ coïncident en tout réel x donc sont égales : $u(\lambda f+\mu g)=\lambda u(f)+\mu u(g)$, c'est-à-dire que u est linéaire.

II Opérations sur les applications linéaires

II.1 L'espace vectoriel $\mathscr{L}(E,F)$

Définition. On note $\mathscr{L}(E,F)$ l'ensemble des applications linéaires de E dans F. Si $E=F$, on le note plus simplement $\mathscr{L}(E)$ (au lieu de $\mathscr{L}(E,E)$).

Remarque : $\mathscr{L}(E)$ est donc l'ensemble des endomorphismes de E. Nous en parlerons plus en détail dans le paragraphe II.4.

Remarque : Rappelons (cf. chapitre 28) que si F est un espace vectoriel alors, pour tout ensemble X, F^X est un $\mathbb{K}$-espace vectoriel avec les lois + et . définies de manière analogue à celles sur tout ensemble de fonctions :

$$\forall (f,g)\in\left(F^X\right)^2,\qquad f+g\colon \begin{cases} X \longrightarrow F \\ x \longmapsto f(x)+g(x)\end{cases}$$

et

$$\forall f\in F^X,\qquad \forall \lambda\in\mathbb{K},\qquad \lambda.f\colon \begin{cases} X \longrightarrow F \\ x \longmapsto \lambda.f(x)\end{cases}$$

et cela munit F^X d'une structure d'espace vectoriel (la structure d'espace vectoriel de F^X vient de celle de F, seul compte le fait que l'ensemble d'arrivée soit un espace vectoriel).

Proposition. $\mathscr{L}(E,F)$ est un $\mathbb{K}$-espace vectoriel.

En particulier, $\mathscr{L}(E,F)$ est stable par CL : une CL d'applications linéaires est encore une application linéaire.

Démonstration. Il suffit donc de prouver que c'est un sev de F^E, qui est un espace vectoriel d'après ce qui précède.

- L'application nulle (de E dans F) est évidemment une application linéaire donc $\mathscr{L}(E,F)$ est non vide.
- Soient $(u,v)\in\mathscr{L}(E,F)^2$ et $(\alpha,\beta)\in\mathbb{K}^2$. Soient enfin $(x,y)\in E^2$ et $(\lambda,\mu)\in\mathbb{K}^2$.

$$\begin{aligned} (\alpha u+\beta v)(\lambda x+\mu y) &= \alpha u(\lambda x+\mu y)+\beta v(\lambda x+\mu y) \\ &= \alpha(\lambda u(x)+\mu u(y))+\beta(\lambda v(x)+\mu v(y)) \\ &= \lambda(\alpha u(x)+\beta v(x))+\mu(\alpha u(y)+\beta v(y)) \\ &= \lambda(\alpha u+\beta v)(x)+\mu(\alpha u+\beta v)(y) \end{aligned}$$

si bien que $\alpha u+\beta v$ est linéaire donc appartient à $\mathscr{L}(E,F)$: $\mathscr{L}(E,F)$ est stable par CL, c'est un sev de F^E. □

II.2 Bijection réciproque

Proposition. Soit $u : E \to F$ un isomorphisme. Alors u^{-1} est linéaire.

En d'autres termes, la bijection réciproque d'une AL bijective est elle-même linéaire.

Démonstration. On rappelle que u^{-1} (bien définie car u est bijective) est l'application :

$$u^{-1} : \begin{cases} F & \to & E \\ y & \mapsto & \text{l'unique } x \in E \text{ tel que } u(x) = y \end{cases}$$

Soient $(y_1, y_2) \in F^2$ et $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. On note $x_1 = u^{-1}(y_1)$ et $x_2 = u^{-1}(y_2)$. Ainsi, $u(x_1) = y_1$ et $u(x_2) = y_2$ donc, par linéarité de u :

$$\begin{aligned} u(\lambda_1 x_1 + \lambda_2 x_2) &= \lambda_1 u(x_1) + \lambda_2 u(x_2) \\ &= \lambda_1 y_1 + \lambda_2 y_2 \end{aligned}$$

En d'autres termes, $\lambda_1 x_1 + \lambda_2 x_2$ est l'unique antécédent de $\lambda_1 y_1 + \lambda_2 y_2$ par u c'est-à-dire que

$$\begin{aligned} u^{-1}(\lambda_1 y_1 + \lambda_2 y_2) &= \lambda_1 x_1 + \lambda_2 x_2 \\ &= \lambda_1 u^{-1}(y_1) + \lambda_2 u^{-1}(y_2) \end{aligned}$$ □

u^{-1} est bien linéaire.

Proposition. Soit $u \in \mathscr{L}(E, F)$. S'il existe $v \in \mathscr{L}(F, E)$ tel que

$$u \circ v = \mathrm{Id}_F \qquad \text{et} \qquad v \circ u = \mathrm{Id}_E$$

alors u est un isomorphisme et $v = u^{-1}$.

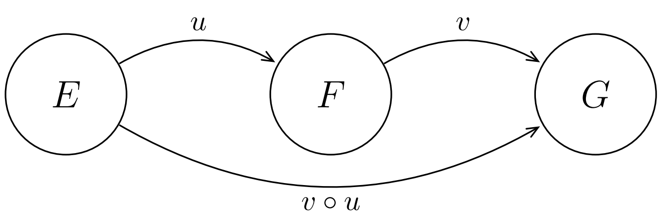
En dimension finie (cf chapitre 30), il suffira d'avoir l'une des deux égalités ci-dessus, mais dans le cas général (cf TD), il faut les deux ! Voir par exemple l'exercice 47 : il est possible d'avoir $u \circ v = \mathrm{Id}_F$ sans que u soit bijective !

Démonstration. Déjà faite dans le chapitre 4.

II.3 Composition d'applications linéaires

Proposition. Soient $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, G)$. Alors $v \circ u \in \mathscr{L}(E, G)$.

Remarque : En d'autres termes, quand elle est bien définie, une composée d'applications linéaires est une application linéaire.



Démonstration. Puisque $v \circ u$ va de E dans G, il suffit de prouver qu'elle est linéaire. Soient $(x, y) \in E^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Tout d'abord,

$$v \circ u(\lambda x + \mu y) = v(u(\lambda x + \mu y))$$

u étant linéaire :

$$v \circ u(\lambda x + \mu y) = v(\lambda u(x) + \mu u(y))$$

v étant linéaire :

$$\begin{aligned} v \circ u(\lambda x + \mu y) &= \lambda v(u(x)) + \mu v(u(x)) \\ &= \lambda v \circ u(x) + \mu v \circ u(x) \end{aligned} \qquad \square$$

donc $v \circ u$ est linéaire.

Proposition. Soient $(v, w) \in \mathscr{L}(E, F)^2, u \in \mathscr{L}(F, G)$. Alors

$$u \circ (v + w) = u \circ v + u \circ w$$

Démonstration. Soit $x \in E$.

$$\begin{aligned} u \circ (v + w)(x) &= u(v(x) + w(x)) \\ &= u(v(x)) + u(w(x)) \\ &= (u \circ v + u \circ w)(x) \end{aligned} \qquad \square$$

La deuxième ligne vient du fait que u est linéaire. Puisque $u \circ (v + w)$ et $u \circ v + u \circ w$ coïncident en tout x, ces deux applications sont égales.

Remarques :

- Par conséquent, la composition est distributive à gauche par rapport à la somme (quand tout est bien défini évidemment).
- Elle est de plus distributive à droite par rapport à la somme, c'est-à-dire que si $w \in \mathscr{L}(E, F)$ et $(u, v) \in \mathscr{L}(F, G)^2$, alors

  $$(u + v) \circ w = u \circ w + v \circ w$$

  mais cette égalité est vraie pour toutes fonctions u, v, w, pas seulement pour des applications linéaires, tandis que la proposition ci-dessus est fausse en général si les applications ne sont pas linéaires.
- Par linéarité, on peut en plus « sortir les constantes », c'est-à-dire :

  Proposition. Soient $(v, w) \in \mathscr{L}(E, F)^2, u \in \mathscr{L}(F, G), (\lambda, \mu) \in \mathbb{K}^2$. Alors

  $$u \circ (\lambda v + \mu w) = \lambda(u \circ v) + \mu(u \circ w)$$

Par exemple, pour tout $x \in \mathbb{R}$, alors

$$\begin{aligned} & (\cos + \sin)(e^x) \\ = \; & \cos(e^x) + \sin(e^x) \end{aligned}$$

c'est-à-dire que

$$\begin{aligned} & (\cos + \sin) \circ \exp \\ = \; & \cos \circ \exp + \sin \circ \exp \end{aligned}$$

alors qu'on n'a pas $\exp \circ (\cos + \sin) = \exp \circ \cos + \exp \circ \sin$ (par exemple en 0, ces deux fonctions ne sont pas égales).

Démonstration. ⇝ Exercice.

Remarques :

- On peut évidemment généraliser à une CL de plus de deux applications linéaires, par une récurrence immédiate.
- Comme dit précédemment, c'est également vrai à gauche, mais c'est le cas pour toutes les fonctions (quand tout est bien défini), pas seulement les applications linéaires.
- On dit que la composition est bilinéaire (cf. chapitres 33 et 34). En clair, cela signifie qu'on peut développer avec une composition comme avec un produit :

  $$(\lambda_1 f_1 + \lambda_2 f_2) \circ (\mu_1 g_1 + \mu_2 g_2) = \lambda_1 \mu_1 (f_1 \circ g_1) + \lambda_2 \mu_1 (f_2 \circ g_1) + \lambda_1 \mu_2 (f_1 \circ g_2) + \lambda_2 \mu_2 (f_2 \circ g_2)$$

- On peut évidemment généraliser à une somme quelconque, et on développe comme pour des sommes de réels classiques (⚠ on change les indices en développant) :

$$\left(\sum_{i=1}^{n} \lambda_i f_i\right) \circ \left(\sum_{i=1}^{p} \mu_i g_i\right) = \sum_{i=1}^{n} \sum_{k=1}^{p} \lambda_i \mu_k (f_i \circ g_k)$$

- Précisons que, par définition de la fonction nulle, $0_{\mathscr{L}(E)} \circ u = 0_{\mathscr{L}(E)}$ et qu'on a également $u \circ 0_{\mathscr{L}(E)} = 0_{\mathscr{L}(E)}$. Cette dernière égalité n'est cependant vraie que parce que u est linéaire ! En effet, une application linéaire est nulle en 0 !
- Rappelons enfin que la composition est associative.
- En clair : la composition, par rapport à la somme, vérifie les mêmes propriétés que le produit sur $\mathbb{R}$ (sauf la commutativité, voir ci-dessous). Ainsi, on écrira parfois vu au lieu de $v \circ u$. Aucune confusion n'est possible avec $v \times u$ puisque le produit n'est pas défini.

Ci-contre, nous n'explicitons pas les notations car elles sont assez transparentes : les f_i sont des AL de F dans G et les g_i des AL de E dans F. Quant aux λ_i et μ_i, ce sont évidemment des scalaires.

Rappelons qu'en général, un espace vectoriel n'est pas muni d'une multiplication.

II.4 L'anneau $\mathscr{L}(E)$: un anneau comme les autres

II.4.a L'anneau proprement dit

Théorème. $(\mathscr{L}(E), +, \circ)$ est un anneau.

DÉMONSTRATION. On sait que $(\mathscr{L}(E), +, .)$ est un $\mathbb{K}$-espace vectoriel donc $(\mathscr{L}(E), +)$ est un groupe abélien. De plus, on sait que la composition est associative et distributive par rapport à la somme (cf. paragraphe précédent). Enfin, Id_E est un élément neutre pour la composition, ce qui permet de conclure.

Remarques :

- ⚠ Il n'est en général pas commutatif : plus précisément, il n'est pas commutatif dès que E est de dimension (finie) supérieure ou égale à 2 (cf. chapitre 30).
- ⚠ Ce n'est pas non plus un anneau intègre en général (voir la suite).
- ⚠ Attention, on rappelle qu'en général, il n'y a pas de multiplication sur un espace vectoriel : par conséquent, $\mathscr{L}(E)$ est un anneau muni de l'addition et de la composition des fonctions, mais pas de l'addition et du produit (ce qui n'aurait de toute façon aucun sens sur $\mathscr{L}(E)$).
- Comme dans tout anneau (cf. chapitre 18), on peut définir la notion de puissance, il existe un binôme de Newton (lorsque les éléments commutent), on peut parler d'éléments nilpotents, d'éléments inversibles etc. Mais, comme dans le chapitre 21, cet anneau revenant très souvent, nous allons revoir tout cela en détail dans le paragraphe suivant.

II.4.b Puissances d'un endomorphisme

Définition. Soit $u \in \mathscr{L}(E)$ et soit $p \in \mathbb{N}^*$. On pose $u^p = \underbrace{u \circ u \circ \cdots \circ u}_{p \text{ fois}}$.

On utilise sans le dire l'associativité de la composition.

Remarques :

- Par convention, on pose $u^0 = \mathrm{Id}_E$.
- D'après le paragraphe précédent, $u^n \in \mathscr{L}(E)$ pour tout n.
- On ne peut définir cette notation que pour des endomorphismes, pas pour des AL quelconques. En effet, si $u \in \mathscr{L}(E, F)$ avec $E \neq F$ alors $u \circ u$ n'est pas défini.
- Cette notation n'est toujours pas gênante car il n'y a aucune notion de produit dans l'espace vectoriel E, on ne risque donc pas de confondre $u^2(x) = u(u(x))$ avec $u(x) \times u(x)$ qui n'est pas défini.

- $u^2 = u \circ u \in \mathscr{L}(E)$. En particulier, $u^2(x) = u(u(x))$. On compose des endomorphismes, pas des vecteurs, écrire $u^2(x) = u(x) \circ u(x)$ n'aurait aucun sens.
- On peut travailler avec la composition comme avec le produit sur $\mathbb{R}$, **à une (grosse) exception près** : LA COMPOSITION N'EST PAS COMMUTATIVE !!! En général, $u \circ v \neq v \circ u$!

Définition. Soient u et $v \in \mathscr{L}(E)$. Si $u \circ v = v \circ u$, on dit que u et v commutent.

Dès lors, « commuter »=« commuter pour la composition ». Puisqu'on vous dit qu'il n'y a pas de produit !

Exemple : Id_E et plus généralement les homothéties (ie les endomorphismes de la forme $\alpha \mathrm{Id}_E$) commutent avec tous les endomorphismes de E ie avec tous les éléments de E.

Proposition. Soient $u \in \mathscr{L}(E)$ et $(p_1, p_2) \in \mathbb{N}^2$.

- $u^{p_1} \circ u^{p_2} = u^{p_2} \circ u^{p_1} = u^{p_1+p_2}$.
- $(u^{p_1})^{p_2} = (u^{p_2})^{p_1} = u^{p_1 \times p_2}$.

Démonstration. Découle de la définition. En particulier, deux puissances d'un même endomorphisme commutent.

II.4.c Binômes de Newton et identités remarquables

Remarque : ⚠ Attention, tous les résultats sur les puissances réelles ou complexes ne sont pas valables pour les endomorphismes ! Par exemple, en général, si u et v appartiennent à $\mathscr{L}(E)$, $(u \circ v)^2 \neq u^2 v^2$! En effet, $(uv)^2 = uvuv$ et $u^2 v^2 = uuvv$. Or, si u et v ne commutent pas, on n'a pas forcément $u \circ v \circ u \circ v = u \circ u \circ v \circ v$! Plus généralement, on n'a pas forcément $(u \circ v)^k = u^k \circ v^k$ lorsque $k \in \mathbb{N}$! En effet :

Rappelons qu'on note parfois uv pour $u \circ v$.

$$(u \circ v)^k = \underbrace{(u \circ v) \circ (u \circ v) \circ \cdots \circ (u \circ v)}_{k \text{ fois}} \qquad \text{et} \qquad u^k v^k = \underbrace{u \circ \cdots \circ u}_{k \text{ fois}} \circ \underbrace{v \circ \cdots \circ v}_{k \text{ fois}}$$

et ces deux quantités n'ont aucune raison d'être égales. De la même façon, les identités remarquables ou (ce qui revient au même) la formule du binôme de Newton ou la formule de factorisation de $a^n - b^n$ ne se généralisent pas sans prendre de gants. Sans hypothèse supplémentaire, tout ce qu'on peut affirmer est que

$$\begin{aligned} (u+v)^2 &= (u+v) \circ (u+v) \\ &= u^2 + u \circ v + v \circ u + v^2 \end{aligned}$$

mais $u \circ v \neq v \circ u$ en général donc on ne peut pas simplifier. De même, sans hypothèse supplémentaire, tout ce qu'on peut affirmer est que

$$(u+v) \circ (u-v) = u^2 - u \circ v + v \circ u - v^2$$

De même, $(u+v)^3 = (u+v)(u+v)(u+v)$ et, par distributivité de la composition sur la somme, on obtient (exo) que $(u+v)^3 = u^3 + u^2 \circ v + u \circ v \circ u + u \circ v^2 + v \circ u^2 + v \circ u \circ v + v^2 \circ u + v^3$ et on ne peut pas faire mieux ! Morale de l'histoire : on peut toujours développer, mais si les endomorphismes ne commutent pas, c'est gore...

et on ne peut pas aller plus loin sans hypothèse supplémentaire. En clair : on peut développer $(u+v)^2$ et plus généralement $(u+v)^k$ et $(u+v) \circ (u-v)$, mais on ne peut pas regrouper les termes donc les formules bien connues ne sont pas valables sans une hypothèse supplémentaire : le fait que les endomorphismes commutent. Comme sur un anneau quelconque, le fait que les deux éléments commutent est une hypothèse indispensable.

Lemme. Soient u et v dans $\mathscr{L}(E)$ qui commutent. Alors, pour tout $k \in \mathbb{N}$, u et v^k commutent.

Démonstration. Par récurrence sur k : $\rightsquigarrow$ Exercice.

Remarque : Plus généralement, toute puissance de u commute avec toute puissance de v .

Il suffit d'appliquer ce lemme avec $\ell \in \mathbb{N}$, v et u^ℓ (au lieu de k, v et u).

Proposition. Soient u et v dans $\mathscr{L}(E)$ qui commutent. Alors, pour tout $k \in \mathbb{N}$, $(u \circ v)^k = u^k \circ v^k$.

Démonstration. ⇝ Exercice.

Proposition (formule du binôme de Newton). Soient u et v deux endomorphismes de E qui **commutent**. Alors, pour tout $p \in \mathbb{N}$,

$$(u+v)^p = \sum_{k=0}^{p} \binom{p}{k} u^k \circ v^{p-k}.$$

Comme dit ci-dessus et dans le chapitre 18, l'hypothèse que u et v commutent est indispensable.

Démonstration. Analogue à celle du chapitre 18.

Théorème. Soient $p \in \mathbb{N}^*$ et $(u,v) \in \mathscr{L}(E)^2$ qui **commutent**. Alors :

$$u^p - v^p = (u-v) \times \left(\sum_{k=0}^{p-1} u^k \circ v^{p-1-k} \right)$$

Démonstration. Idem, analogue au chapitre 18.

Corollaire. Soient $p \in \mathbb{N}^*$ et $u \in \mathscr{L}(E)$. Alors :

$$\mathrm{Id}_E - u^p = (\mathrm{Id}_E - u) \circ \sum_{k=0}^{p-1} u^k$$

Démonstration. Immédiat puisque Id_E et u commutent.

II.4.d Endomorphismes nilpotents

Définition. Soit $u \in \mathscr{L}(E)$. On dit que u est nilpotent s'il existe $p \in \mathbb{N}$ tel que $u^p = 0_{\mathscr{L}(E)}$ c'est-à-dire tel que u^p soit l'application nulle. Le plus petit entier p qui vérifie cette condition est appelé l'indice de nilpotence de u.

En d'autres termes, un endomorphisme nilpotent est une application linéaire qui « devient nulle » dès qu'on l'applique un certain nombre de fois.

Exemples :

- L'application

$$u : \begin{cases} \mathbb{K}^2 & \longrightarrow & \mathbb{K}^2 \\ (x,y) & \longmapsto & (y,0) \end{cases}$$

est nilpotente d'indice de nilpotence 2. En effet, elle est linéaire (exo), $u(0,1) = (1,0) \neq 0$ et pour tout $(x,y) \in \mathbb{K}^2$,

$$\begin{aligned} u^2(x,y) &= u(u(x,y)) \\ &= u(y,0) \\ &= (0,0) \end{aligned}$$

Pour prouver que u est nilpotente d'indice de nilpotence 2, il faut prouver que u est linéaire, que $u^2 = 0$ et $u \neq 0$.

puisque, par définition :

$$u(\text{première coordonnée}, \text{deuxième coordonnée}) = (\text{deuxième coordonnée}, 0)$$

- Si $n \geqslant 0$, l'application

$$D: \begin{cases} \mathbb{K}_n[X] \longrightarrow \mathbb{K}_n[X] \\ \quad P \quad \longmapsto \quad P' \end{cases}$$

est nilpotente d'indice de nilpotence $n+1$. En effet, elle est linéaire (cf. paragraphe IV.4), pour tout $P \in \mathbb{K}_n[X]$,

$$D^{n+1}(P) = P^{(n+1)} = 0$$

et $D^n(X^n) = (X^n)^{(n)} = n! \neq 0$.

- ⚠ L'application

$$D: \begin{cases} \mathbb{K}[X] \longrightarrow \mathbb{K}[X] \\ \quad P \quad \longmapsto \quad P' \end{cases}$$

n'est pas nilpotente (alors que, pour tout n, sa restriction à $\mathbb{K}_n[X]$ l'est) même si, pour tout p, il existe n tel que $D^n(P) = 0$. La raison est que le n dépend de P : pour annuler P, il faut le dériver un nombre de fois strictement supérieur à son degré, ce qui n'est pas le cas sur $\mathbb{K}_n[X]$, où il suffit de dériver $n+1$ fois pour annuler tout le monde. En effet, rappelons que la définition de la nilpotence est :

$$\exists n \geqslant 1, \forall P \in \mathbb{K}[X], D^n(P) = 0$$

c'est-à-dire qu'il faut le même exposant pour tout le monde. La négation est :

$$\forall n \geqslant 1, \exists P \in \mathbb{K}[X], D^n(P) \neq 0$$

Or, pour tout $n \geqslant 1$, si on prend P de degré n de coefficient dominant $a_n \neq 0$, alors $D^n(P) = P^{(n)} = n! \times a_n \neq 0$: D n'est pas nilpotente.

Cet exemple peut sembler un peu artificiel, mais ce sera notre exemple type d'endomorphisme nilpotent dans le chapitre 31. Géométriquement, il correspond à la composée (dans cet ordre) de la projection sur l'axe des ordonnées suivie d'une rotation d'angle $-\pi/2$ de centre l'origine : en l'appliquant deux fois, on tombe forcément sur 0.

⚠ Exemple classique !

Proposition. Soit $u \in \mathscr{L}(E)$ nilpotent d'indice p. Alors : $\forall k \geqslant p, u^k = 0_{\mathscr{L}(E)}$.

Démonstration. Soit $k \geqslant p$. Alors

$$\begin{aligned} u^k &= u^p \circ u^{k-p} \\ &= 0_{\mathscr{L}(E)} \circ u^{k-p} \\ &= 0_{\mathscr{L}(E)} \end{aligned}$$

□

Proposition. Soient $(u_1, u_2) \in \mathscr{L}(E)^2$ nilpotents qui **commutent**. Alors $u_1 \circ u_2$ est nilpotente.

Démonstration. Notons p_1 l'indice de nilpotence de u_1 et p_2 celui de u_2. Soit $p = \max(p_1, p_2)$. Puisque u_1 et u_2 commutent, alors : $(u_1 \circ u_2)^p = {u_1}^p \circ {u_2}^p$. Or, $p \geqslant p_1$ donc ${u_1}^p = 0$ et, de même, ${u_2}^p = 0$ donc $(u_1 \circ u_2)^p = 0$.

Remarque : ⚠ C'est faux si les deux endomorphismes ne commutent pas.

Proposition. Soient $(u_1, u_2) \in \mathscr{L}(E)^2$ nilpotents qui **commutent**. Alors $u_1 + u_2$ est nilpotent.

Résultat classique mais HP : à savoir redémontrer !

DÉMONSTRATION. Notons p_1 l'indice de nilpotence de u_1 et p_2 celui de u_2. Montrons que $(u_1+u_2)^{p_1+p_2-1} = 0_{\mathscr{L}(E)}$. Les endomorphismes u_1 et u_2 commutent donc, d'après le binôme de Newton :

$$(u_1+u_2)^{p_1+p_2-k} = \sum_{k=0}^{p_1+p_2-1} \binom{p_1+p_2-1}{k} {u_1}^k \circ {u_2}^{p_1+p_2-1-k}$$

□

Soit $k \in [\![0\,; p_1+p_2-1]\!]$.

- Si $k \geqslant p_1$ alors ${u_1}^k = 0$.
- Si $k < p_1$ alors $p_1+p_2-1-k > p_2 - 1$ donc $p_1+p_2-1-k \geqslant p_2$. En particulier, ${u_2}^{p_1+p_2-1-k} = 0$.

Finalement, tous les termes de la somme sont nuls : $(u_1+u_2)^{p_1+p_2-1} = 0_{\mathscr{L}(E)}$, l'endomorphisme u_1+u_2 est bien nilpotent.

Remarque : ⚠ C'est faux si les deux endomorphismes ne commutent pas !

Nous donnerons des exemples dans le chapitre 31.

II.4.e Le groupe $\mathrm{GL}(E)$

Définition. L'ensemble des automorphismes de E est noté $\mathrm{GL}(E)$ et est appelé groupe linéaire.

Remarques :

- En d'autres termes, c'est l'ensemble des endomorphismes bijectifs de E, c'est-à-dire l'ensemble des éléments inversibles (pour la loi $\circ$) de l'anneau $\mathscr{L}(E)$: c'est donc bien un groupe car on sait (cf. chapitre 18) que l'ensemble des inversibles d'un anneau est un groupe pour la deuxième loi (ici, la composition). En particulier, si u et v appartiennent à $\mathrm{GL}(E)$, leur composée $u \circ v$ également.
- L'écriture $\mathrm{GL}(E)$ et sa ressemblance avec $\mathrm{GL}_n(\mathbb{K})$ n'est pas un hasard, il y a un lien étroit entre ces ensembles : cf. chapitre 31.

Exemples :

- Une homothétie de rapport non nul est un automorphisme.
- Un endomorphisme nilpotent n'est jamais injectif donc n'est jamais bijectif. En effet, si u est un endomorphisme nilpotent, alors, si on note p son indice de nilpotence, alors $u^p = 0$ donc u^p n'est pas injectif donc u n'est pas injectif (en effet, une composée de fonctions injectives est injective, donc si u est injective, alors u^p est injective donc on a le résultat par contraposée). Cependant, de manière analogue aux chapitres 18 et 21, on peut montrer que $\mathrm{Id}_E - u$ est inversible, d'inverse $\displaystyle\sum_{k=0}^{p-1} u^k$: $\rightsquigarrow$ EXERCICE..
- On peut étendre la notation puissance aux entiers négatifs dans le cas des automorphismes :

Définition. Soit $u \in \mathrm{GL}(E)$ et soit $p \in \mathbb{Z}, p < 0$. On pose

$$u^p = \underbrace{u^{-1} \circ u^{-1} \circ \cdots \circ u^{-1}}_{-p \text{ fois}}$$

Remarques :

- Par exemple,

$$u^{-3} = \underbrace{u^{-1} \circ u^{-1} \circ u^{-1}}_{3 \text{ fois}}$$

- Là aussi, cette notation vérifie les mêmes conditions que la notation puissance sur $\mathbb{R}$.
- Cette notation n'a de sens que sur $\mathrm{GL}(E)$ puisque u^{-1} n'existe que si u est bijectif.

III Noyau et image

III.1 Image

Lemme. Soient $u \in \mathscr{L}(E, F)$, E_1 un sev de E et F_1 un sev de F. Alors $u(E_1)$ est un sev de F et $u^{-1}(F_1)$ est un sev de E.

Remarques :

- En d'autres termes, l'image directe ou réciproque d'un sev par une application linéaire est encore un sev (de l'espace de départ ou d'arrivée, selon qu'on s'intéresse à une image directe ou une image réciproque). Les applications linéaires, dans un sens comme dans l'autre, préservent la structure.
- Il n'est supposé nulle part que u est bijective. Rappelons qu'on peut toujours définir l'image réciproque d'un ensemble par une application, c'est l'ensemble des éléments dont l'image appartient à cet ensemble :

$$u^{-1}(F_1) = \{x \in E \,|\, u(x) \in F_1\}$$

En particulier, avec des quantificateurs : $x \in u^{-1}(F_1) \iff u(x) \in F_1$.

Démonstration.
- $0_E \in E_1$ et $u(0_E) = 0_F$ donc $0_F \in u(E_1)$: $u(E_1)$ est non vide.
- Soient $(y_1, y_2) \in u(E_1)^2$, $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. Il existe $(x_1, x_2) \in {E_1}^2$ tels que $y_1 = u(x_1), y_2 = u(x_2)$. On a :

$$\begin{aligned} \lambda_1 y_1 + \lambda_2 y_2 &= \lambda_1 u(x_1) + \lambda_2 u(x_2) \\ &= u(\lambda_1 x_1 + \lambda_2 x_2) \end{aligned}$$

par linéarité de u. Or, E_1 est un sev de E donc est stable par CL : $\lambda_1 x_1 + \lambda_2 x_2 \in E_1$. Finalement, $\lambda_1 y_1 + \lambda_2 y_2 \in u(E_1)$: $u(E_1)$ est un sev de F.

Passons à présent à $u^{-1}(F_1)$.

- $u(0_E) = 0_F \in F_1$ puisque F_1 est un sev de F donc $0_E \in u^{-1}(F_1)$: $u^{-1}(F_1)$ est non vide.
- Soient $(x_1, x_2) \in u^{-1}(F_1)^2$, $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. Par linéarité de u,

$$u(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 u(x_1) + \lambda_2 u(x_2) \qquad \square$$

Or, F_1 est un sev de F donc est stable par CL, et puisque $u(x_1)$ et $u(x_2)$ appartiennent à F_1, alors $u(\lambda_1 x_1 + \lambda_2 x_2) \in F_1$ si bien que $\lambda_1 x_1 + \lambda_2 x_2$: $u^{-1}(F_1)$ est un sev de E.

Définition. Soit $u \in \mathscr{L}(E, F)$. On note $\mathrm{Im}(u)$ et on appelle image de u l'ensemble $u(E)$ i.e. $\mathrm{Im}(u) = \{u(x) \mid x \in E\}$.

En clair : l'image, c'est l'ensemble des images...

Remarque : Avec des quantificateurs, si $y \in F$:

$$y \in \mathrm{Im}(u) \iff \exists x \in E, y = u(x)$$

Corollaire. Soit $u \in \mathscr{L}(E, F)$. $\mathrm{Im}(u)$ est un sev de F.

Remarque : u est surjective si et seulement si $\mathrm{Im}(u) = F$.

III.2 Noyau

Définition. Soit $u \in \mathscr{L}(E, F)$. On appelle noyau de u, noté $\ker(u)$, l'ensemble :

$$\ker(u) = \{x \in E \mid u(x) = 0_F\}$$

Remarques :

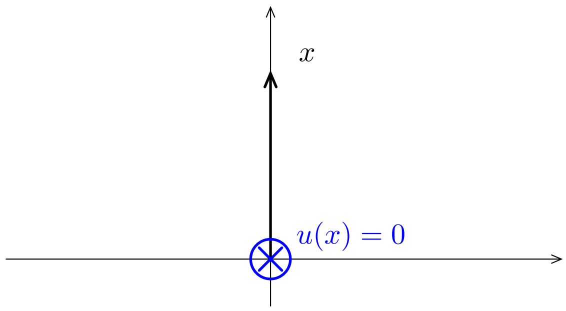
- En d'autres termes, ce sont les éléments d'image nulle par u.
- C'est la même définition que dans le chapitre 18 : les éléments dont l'image est envoyé sur le neutre.

Proposition. Soit $u \in \mathscr{L}(E, F)$. $\ker(u)$ est un sev de E.

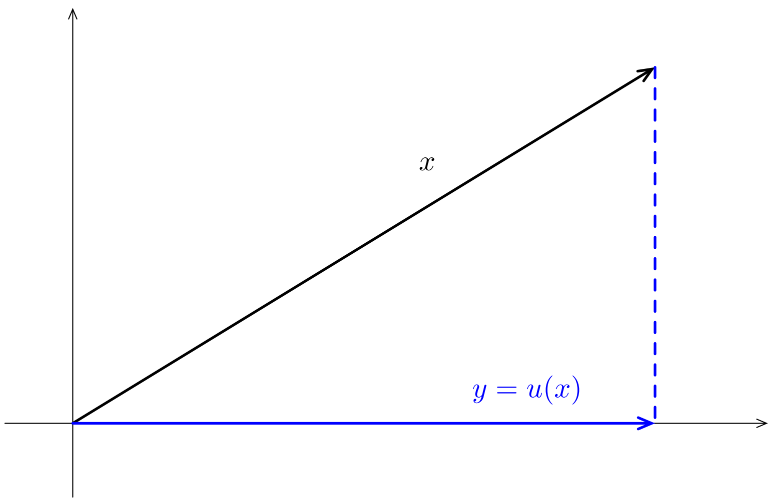
Démonstration. $\ker(u) = u^{-1}\{0_F\}$ et $\{0_F\}$ est un sev de F donc $\ker(u)$ est un sev de E car image réciproque d'un sev de F par une application linéaire.

Exemples :

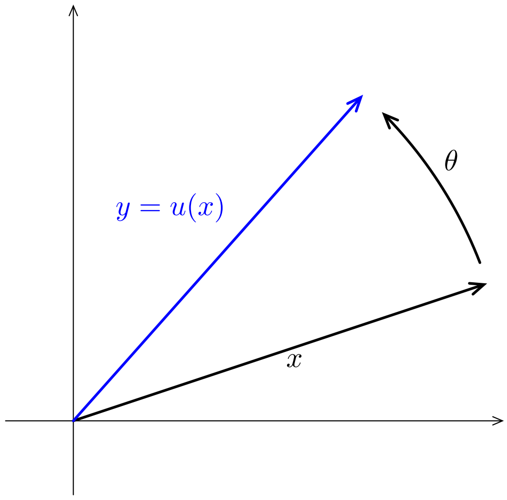
- Dans $\mathbb{R}^2$, soit u la projection orthogonale (encore une fois, il existe des projections non orthogonales, cf III) sur l'axe des abscisses. Le noyau est l'axe des ordonnées :



et l'image est l'axe des abscisses :



- Si u est une rotation dans $\mathbb{R}^2$, son noyau est $\{0\}$ (en effet, si $x \neq 0$ alors $u(x) \neq 0$) et son image est $\mathbb{R}^2$ tout entier : en effet, pour tout $y \in \mathbb{R}^2$, il existe $x \in \mathbb{R}^2$ tel que $u(x) = y$.



- Soit

$$u : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ & & \\ P & \mapsto & P' \end{array} \right.$$

Alors $\ker(u) = \mathbb{R}_0[X]$ c'est-à-dire l'ensemble des polynômes constants, et $\mathrm{Im}(u) = \mathbb{R}[X]$. En effet, soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$. Alors $P = u(Q)$ où $Q = \displaystyle\sum_{k=0}^{n} \frac{a_k}{k+1} \times X^{k+1}$ donc $P \in \mathrm{Im}(u)$.

Encore une fois, nous reparlerons de la dérivée des polynômes en détail dans le paragraphe IV.4.

Proposition. Soit $u \in \mathscr{L}(E, F)$. u est injective si et seulement si $\ker(u) = \{0_E\}$.

Remarque : Ainsi, parmi les exemples précédents, seule la rotation est injective.

Démonstration. Supposons u injective. 0_F admet donc au plus un antécédent par u. Or, $u(0_E) = 0_F$ car u est linéaire donc 0_E est l'unique antécédent de 0_F par u : $\ker(u) = \{0_E\}$.

On l'a déjà faite dans le chapitre 18, mais on la refait pour se familiariser avec la notion d'AL et de noyau.

Réciproquement, supposons que $\ker(u) = \{0_E\}$. Soient $(x_1, x_2) \in E^2$ tels que $u(x_1) = u(x_2)$. Montrons que $x_1 = x_2$. On a $u(x_1) - u(x_2) = 0_F$. u étant linéaire, $u(x_1 - x_2) = 0_F$ donc $x_1 - x_2 \in \ker(u) = \{0_E\}$. Ainsi, $x_1 - x_2 = 0_E$. Finalement, $x_1 = x_2$ donc u est injective.

Remarque : De même que pour deux sous-espaces vectoriels dont on veut montrer qu'ils sont en somme directe, pour montrer qu'une AL u est injective, puisque $\ker(u)$ est un sev de E, on se contentera de montrer l'inclusion $\ker(u) \subset \{0_E\}$, l'inclusion réciproque étant toujours vraie.

Exemple : Soit

$$u : \left\{ \begin{array}{ccc} \mathscr{C}(\mathbb{R}, \mathbb{R}) & \to & \mathscr{C}(\mathbb{R}, \mathbb{R}) \\ & & \\ f & \mapsto & f \times \sin \end{array} \right.$$

Soient $(f, g) \in \mathscr{C}(\mathbb{R}, \mathbb{R})^2$ et $(\lambda, \mu) \in \mathbb{R}^2$.

$$\begin{aligned} u(\lambda f + \mu g) &= (\lambda f + \mu g) \times \sin \\ &= \lambda f \times \sin + \mu g \times \sin \\ &= \lambda u(f) + \mu u(g) \end{aligned}$$

c'est-à-dire que u est linéaire. Montrons que u est injective. Soit $f \in \ker(u)$. Alors $f \times \sin = 0$ (la fonction nulle), c'est-à-dire que pour tout $x \in \mathbb{R}, f(x) \times \sin(x) = 0$ (le réel 0). Par conséquent, f est nulle sur $\mathbb{R} \backslash \pi\mathbb{Z}$. La fonction f étant continue, elle est nulle sur $\mathbb{R}$. $\ker(u) = \{0\}$: u est injective.

IV AL et familles de vecteurs

IV.1 Détermination d'une AL : « rigidité » des applications linéaires

De façon générale, deux fonctions u et v définies sur un même ensemble E sont égales si elles coïncident en tout élément de E, c'est-à-dire si $u(x) = v(x)$ pour tout élément x de E. On va voir que cette condition peut être considérablement affaiblie quand u et v sont des applications linéaires.

On sait que si c est un réel non nul et si d est un réel (qui peut être nul), il existe une unique fonction $f : \mathbb{R} \to \mathbb{R}$ linéaire telle que $f(c) = d$. On veut généraliser ce résultat.

De façon explicite :

$$f : x \mapsto \frac{d}{c} \times x$$

Théorème. Soient $(e_i)_{i\in I}$ une base de E et $(f_i)_{i\in I}$ une famille quelconque d'éléments de F (pas forcément une base). Alors il existe une unique application linéaire $u \in \mathscr{L}(E, F)$ telle que $u(e_i) = f_i$ pour tout $i \in I$. Ainsi une AL de E dans F est entièrement déterminée par l'image d'une base.

Remarque : Ce résultat généralise bien celui de la remarque précédente puisqu'un réel non nul c est une base de $\mathbb{R}$. Il stipule donc qu'il suffit de connaître l'image d'une base pour connaître l'image de tout vecteur, ce qui est intuitif par linéarité. Plus fort : une telle application linéaire existe forcément (et donc est forcément unique d'après ce qui précède), ce qui se conçoit par exemple très bien avec les exemples vus précédemment (cf. paragraphe I.1) :

- il suffit de connaître l'image de x_1 et x_2 pour connaître l'image de tout élément de $\text{Vect}(x_1, x_2)$.
- Il suffit de connaître l'image de $x_1, \dots, x_n$ pour connaître l'image de tout élément de $\text{Vect}(x_1, \dots, x_n)$.
- Sur $\mathbb{K}[X]$: il suffit de savoir que la dérivée de tout polynôme de la forme X^n est nX^{n-1} pour dériver n'importe quel polynôme : cf. paragraphe I.1.

Si on est sur une famille génératrice mais pas sur une base, certains vecteurs peuvent se voir affecter « plusieurs valeurs » : si celles-ci sont égales, aucun problème, sinon... c'est qu'une telle application n'existe pas !

cf. exercice 28.

DÉMONSTRATION. Par analyse-synthèse.

- **Analyse :** Si u convient. Soit $x \in E$. $(e_i)_{i\in I}$ étant une base de E, il existe une unique $(\alpha_i)_{i\in I}$ une famille presque nulle de scalaires telle que $x = \displaystyle\sum_{i\in I} \alpha_i e_i$. u étant linéaire,

$$\begin{aligned} u(x) &= \sum_{i\in I} \alpha_i u(e_i) \\ &= \sum_{i\in I} \alpha_i f_i \end{aligned}$$

En d'autres termes, u est la fonction

$$\left\{ \begin{array}{ccc} E & \to & F \\ \displaystyle\sum_{i\in I} \alpha_i e_i & \mapsto & \displaystyle\sum_{i\in I} \alpha_i f_i \end{array} \right.$$

où $(\alpha_i)_{i\in I}$ est une famille presque nulle de scalaire.

- **Synthèse :** Soit

$$\left\{\begin{array}{ccc} E & \to & F \\ \displaystyle\sum_{i\in I}\alpha_i e_i & \mapsto & \displaystyle\sum_{i\in I}\alpha_i f_i \end{array}\right.$$

où $(\alpha_i)_{i\in I}$ est une famille presque nulle de scalaire. Cela définit bien une fonction car tout élément de E s'écrit d'une façon unique comme combinaison linéaire des e_i (et donc, si on a une telle combinaison linéaire, c'est la bonne et on peut donner directement l'image par u). Montrons que u convient, c'est-à-dire que u est linéaire et que $u(e_i) = f_i$ pour tout $i \in I$. Soit donc $i \in I$. $e_i = 1.e_i$ donc $u(e_i) = 1.f_i$ ie $u(e_i) = f_i$: la deuxième condition est vérifiée. Soient $(x, y) \in E^2$. Il existe deux uniques familles presque nulles de scalaires $(\alpha_i)_{i\in I}$ et $(\beta_i)_{i\in I}$ telles que

$$x = \sum_{i\in I}\alpha_i e_i \qquad \text{et} \qquad y = \sum_{i\in I}\beta_i e_i$$

Dès lors,

$$x + y = \sum_{i\in I}(\alpha_i + \beta_i)e_i$$

Par définition de u :

$$\begin{aligned} u(x+y) &= \sum_{i\in I}(\alpha_i+\beta_i)f_i \\ &= \sum_{i\in I}\alpha_i f_i + \sum_{i\in I}\beta_i f_i \\ &= u(x) + u(y) \end{aligned}$$

□

On montre de même que, pour tout $\lambda \in \mathbb{K}, u(\lambda x) = \lambda u(x)$: u est bien linéaire.

On passe sous silence le fait que $(\alpha_i + \beta_i)_{i\in I}$ soit presque nulle : comme dans le chapitre 6, on prouve que le support de cette famille est inclus dans l'union des supports de $(\alpha)_{i\in I}$ et $(\beta)_{i\in I}$ donc est inclus dans l'union de deux ensembles finis donc est fini. Comme on l'a dit dans le chapitre précédent : on peut manipuler ce genre de somme sans se poser de question.

Exemples : Dans les quatre exemples suivants, on note (e_1, e_2, e_3) la base canonique de $\mathbb{K}^3$.

- Soit $u : \mathbb{K}^3 \to \mathbb{K}^{2024}$ linéaire telle que $u(e_1) = u(e_2) = u(e_3) = 0$. Alors u est l'application nulle. En effet, u et l'application nulle sont deux applications linéaires qui coïncident sur une base donc sont égales.

Raisonnement classique !

- Donner l'unique AL $u : \mathbb{K}^3 \to \mathbb{K}^2$ telle que

$$u(e_1) = (2,3) \qquad u(e_2) = (1,0) \qquad \text{et} \qquad u(e_3) = (3,3)$$

Soit u cette AL (son existence et son unicité découlent du théorème). Soit $x = (x_1, x_2, x_3) \in \mathbb{K}^3$.

$$\begin{aligned} u(x) &= u(x_1e_1 + x_2e_2 + x_3e_3) \\ &= x_1u(e_1) + x_2u(e_2) + x_3u(e_3) \qquad (u \text{ est linéaire}) \\ &= x_1(2,3) + x_2(1,0) + x_3(3,3) \\ &= (2x_1 + x_2 + 3x_3, 3x_1 + 3x_2) \end{aligned}$$

- Donner l'unique AL $u : \mathbb{R}^3 \to \mathbb{R}_4[X]$ vérifiant

$$u(e_1) = X^4 + X + 1 \qquad u(e_2) = 0 \qquad \text{et} \qquad u(e_3) = X^4 + 2X^3 + X + 1$$

De même :

$$\forall x = (x_1, x_2, x_3) \in \mathbb{K}^3, \qquad u(x) = (x_1 + x_3)X^4 + 2x_3X^3 + (x_1 + x_3)X + (x_3 - x_1)$$

- Donner l'unique AL $u : \mathbb{R}^3 \to \mathbb{R}_4[X]$ vérifiant

$$u(e_1) = X + 1 \qquad u(e_2) = X^3 + X + 1 \qquad \text{et} \qquad u(e_3) = X^4$$

Alors :

$$\forall x = (x_1, x_2, x_3) \in \mathbb{K}^3, \qquad u(x) = x_3X^4 + x_2X^3 + (x_1 + x_2)X + (x_1 + x_2)$$

IV.2 Détermination à l'aide de la restriction à deux sev supplémentaires

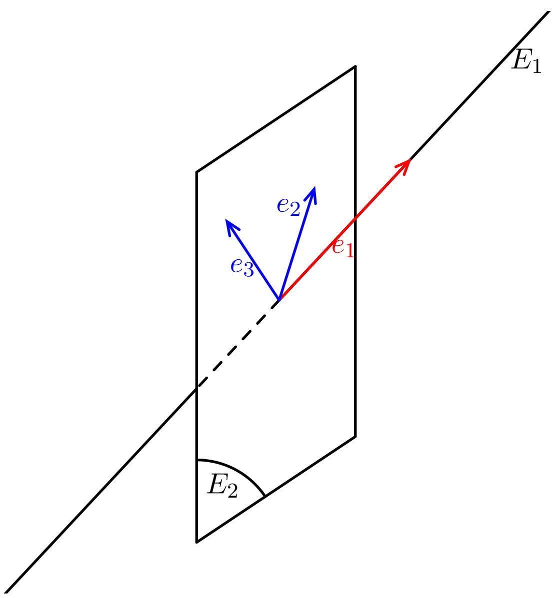
Tout est dans le titre...

Proposition. Soient E_1 et E_2 deux sous-espaces vectoriels supplémentaires de E. Soient $u_1 \in \mathscr{L}(E_1, F)$ et $u_2 \in \mathscr{L}(E_2, F)$. Alors il existe une unique application linéaire $u \in \mathscr{L}(E, F)$ telle que $u_{|E_1} = u_1$ et $u_{|E_2} = u_2$. E d'autres termes, une AL de E dans F est entièrement déterminée par sa restriction à deux sous-espaces supplémentaires.

Démonstration. Par analyse-synthèse, en utilisant le fait que tout élément $x \in E$ peut s'écrire de façon unique comme d'un élément $x_1 \in E_1$ et d'un élément $x_2 \in E_2$: le reste est analogue au paragraphe précédent. $\leadsto$ Exercice.

Remarque : L'idée est analogue à celle du paragraphe précédent : par linéarité, il suffit de connaître u sur « deux morceaux qui engendrent tout l'espace », et si en plus les deux espaces sont supplémentaires, alors il y a existence. Par exemple, ci-dessous, il suffit de connaître u sur E_1 et sur E_2 pour caractériser entièrement u :

Si l'intersection n'est pas nulle, il faut voir si les deux AL u_1 et u_2 sont compatibles i.e. si les deux définitions ne se contredisent pas sur $E_1 \cap E_2$.



IV.3 Image d'une famille libre, d'une famille génératrice, d'une base

Théorème. Soit $u \in \mathscr{L}(E, F)$.

1. Si G est une famille génératrice de E alors $u(G)$ est une famille génératrice de $\mathrm{Im}(u)$. En d'autres termes, l'image d'une famille génératrice est une famille génératrice de l'image.
2. Si S est une famille liée de E alors $u(S)$ est une famille liée de F. En d'autres termes, l'image d'une famille liée est une famille liée.
3. Si L est une famille libre de E **et** si u est injective alors alors $u(L)$ est une famille libre de F. En d'autres termes, l'image d'une famille libre par une application injective est une famille libre.

Démonstration.

1. Soit $y \in \mathrm{Im}(u)$. Il existe $x \in E$ tel que $y = u(x)$. G étant une famille génératrice de E, x est CL des éléments de G c'est-à-dire qu'il existe $e_1, \dots, e_n$ des éléments de G et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ tels que $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$. u étant linéaire,
$$y = \alpha_1 u(e_1) + \cdots + \alpha_n u(e_n)$$
c'est-à-dire que tout élément de $\mathrm{Im}(u)$ est CL d'éléments de $u(G)$, ce qui est le résultat voulu.
2. Notons $S = (e_i)_{i \in I}$. Par hypothèse, il existe une famille de scalaires non tous nuls $(\lambda_i)_{i \in I}$ telle que
$$\sum_{i \in I} \lambda_i e_i = 0$$
Dès lors, $u\left(\sum_{i \in I} \lambda_i e_i\right) = u(0)$. u étant linéaire,
$$\sum_{i \in I} \lambda_i u(e_i) = 0$$
Les λ_i étant non tous nuls, les $u(e_i)$ forment une famille liée.
3. Soit $(e_1, \dots, e_n)$ une sous-famille finie de L. Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ tels que $\lambda_1 u(e_1) + \cdots + \lambda_n u(e_n) = 0$. Par linéarité de u,
$$u(\lambda_1 e_1 + \cdots + \lambda_n e_n) = 0$$
c'est-à-dire que $\lambda_1 e_1 + \cdots + \lambda_n e_n \in \ker(u)$. Or, $\ker(u) = \{0\}$ car u est injective. Ainsi, $\lambda_1 e_1 + \cdots + \lambda_n e_n = 0$. Or, les e_i sont libres donc $\lambda_1 = \cdots = \lambda_n = 0$: les $u(e_i)$ forment une famille libre. Toute sous-famille finie est libre donc $u(L)$ est une famille libre. □

Corollaire. Soit $u \in \mathscr{L}(E, F)$ et soit B une **base** de E.

1. u est injective si et seulement si $u(B)$ est une famille libre.
2. u est surjective si et seulement si $u(B)$ est une famille génératrice.
3. u est bijective si et seulement si $u(B)$ est une base.

Si u est bijective, on dit que u est un isomorphisme : une application linéaire est donc un isomorphisme si et seulement si elle envoie une base sur une base.

Démonstration.

1. On a déjà montré le sens « u injective » $\Rightarrow$ « $u(B)$ famille libre ». Réciproquement, supposons que $u(B)$ soit une famille libre et montrons que u est injective. Soit $x \in \ker(u)$. B étant une base, il existe une famille finie de vecteurs de B qu'on note $e_1, \dots, e_n$ et une famille de scalaires $(\alpha_1, \dots, \alpha_n)$ telles que

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n$$

u étant linéaire,

$$u(x) = \alpha_1 u(e_1) + \cdots + \alpha_n u(e_n)$$

Or, $x \in \ker(u)$ donc $u(x) = 0$ ie

$$\alpha_1 u(e_1) + \cdots + \alpha_n u(e_n) = 0 \qquad \square$$

Les $u(e_i)$ sont libres donc $\alpha_1 = \cdots = \alpha_n = 0$ ie $x = 0$. $\ker(u) = \{0\}$ donc u est injective.

2. Découle du théorème précédent.
3. Conséquence des deux premiers points.

Remarque : Parmi les quatre exemples du paragraphe précédent, seule la deuxième est surjective et seule la dernière est injective.

IV.4 Application aux polynômes

Le but de ce paragraphe est de prouver tous les résultats admis à propos de la dérivation formelle de polynômes vue dans le chapitre 19. Rappelons qu'un polynôme n'est pas une fonction et que, même si on peut confondre la plupart du temps polynôme et fonction polynomiale, si on se place sur un corps différent de $\mathbb{R}$, la notion de dérivée en tant que limite du taux d'accroissement n'est pas définie alors que la notion de dérivée formelle d'un polynôme, elle, est bien définie : on peut par exemple dériver un polynôme complexe sans se poser de question, alors qu'on ne peut pas dériver des fonctions de la variable complexe (on peut dériver des fonctions de $\mathbb{R}$ dans $\mathbb{C}$ mais pas des fonctions de $\mathbb{C}$ dans $\mathbb{C}$).

Les résultats de ce paragraphe ne sont pas valables sur un corps quelconque, uniquement sur ce qu'on appelle un corps de caractéristique nulle, mais puisque le cadre officiel du programme est de se placer sur $\mathbb{R}$ ou $\mathbb{C}$, alors tout va bien.

Définition (Rappel - cf. chapitre 19). Soit $P = \displaystyle\sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. On appelle polynôme dérivé ou dérivée formelle du polynôme P le polynôme noté P' ou $D(P)$ défini par :

$$P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$$

La somme ci-contre est en réalité finie, et on fait parfois commencer la somme en 0, le terme ajouté étant alors nul.

Rappelons que c'est une définition purement arbitraire : on choisit de noter P' ou $D(P)$ un certain polynôme, et on l'appelle polynôme dérivé de P, sans que cette définition ait un lien quelconque a priori avec un quelconque taux d'accroissement.

La raison est que, sur $\mathbb{K} = \mathbb{R}$, la fonction polynomiale associée à P' est la dérivée de la fonction polynomiale associée à P : sur $\mathbb{R}$, « ça marche », et on étend la définition à $\mathbb{K}$.

On avait adopté dans le chapitre 19 le point de vue habituel, c'est-à-dire « fonctionnel » en utilisant le plus souvent la notation P' pour travailler comme avec des fonctions dérivables classiques, et pour renforcer l'analogie polynôme/fonction polynomiale. On va plutôt utiliser ici le point de vue « opérationnel » c'est-à-dire que le polynôme dérivé sera noté $D(P)$. Plus précisément :

Définition. On définit l'opérateur dérivation D par :

$$D : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ \displaystyle\sum_{k=0}^{+\infty} a_k X^k & \longmapsto & \displaystyle\sum_{k=0}^{+\infty} k a_k X^{k-1} = \sum_{k=1}^{+\infty} k a_k X^{k-1} \end{cases}$$

Voir D comme une application linéaire va nous permettre de prouver tous les résultats admis au chapitre 19. En effet :

Proposition. D est une application linéaire de $\mathbb{K}[X]$ dans lui-même.

En d'autres termes, D est un endomorphisme de $\mathbb{K}[X]$.

Démonstration. Faite dans le chapitre 19.

Par conséquent, l'idée de toutes les preuves du paragraphe est la suivante : si on veut prouver un résultat concernant les polynômes, il suffit de le prouver pour les polynômes de la base canonique $(X^n)_{n\in\mathbb{N}}$ puisque, pour caractériser une application linéaire, il suffit de connaître l'image d'une base.

Proposition. Soit $(P,Q)\in\mathbb{K}[X]^2$. Alors $(PQ)'=P'Q+PQ'$.

Démonstration. Avec la notation D, il suffit donc de prouver que $D(PQ)=D(P)Q+PD(Q)$. Soit $n\in\mathbb{N}$. Soient

$$u_1 : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & D(X^nP) \end{cases} \qquad \text{et} \qquad u_2 : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & X^nD(P)+PD(X^n) \end{cases}$$

Prouvons que $u_1=u_2$. D étant linéaire, u_1 et u_2 le sont aussi (exo). Par conséquent, pour prouver qu'elles sont égales, il suffit de prouver qu'elles coïncident sur une base, en l'occurence la base canonique $(X^p)_{p\in\mathbb{N}}$. Si $p=0$, d'une part, $u_1(X^p)=u_1(1)=D(P)$ et, d'autre part, $u_2(X^p)=1\times D(P)+PD(1)=D(P)$ puisque $D(1)=0$. Soit à présent $p\geqslant 1$. D'une part :

$$\begin{aligned} u_1(X^p) &= D(X^{n+p}) \\ &= (n+p)X^{n+p-1} \end{aligned}$$

et d'autre part

$$\begin{aligned} u_2(X^p) &= X^nD(X^p)+X^pD(X^n) \\ &= X^n\times pX^{p-1}+X^p\times nX^{n-1} \\ &= (n+p)X^{n+p-1} \\ &= u_1(X^p) \end{aligned}$$

Par conséquent, u_1 et u_2 coïncident sur une base donc sont égales, et n étant quelconque, on a prouvé le résultat suivant :

$$\forall n\in\mathbb{N}, \forall P\in\mathbb{K}[X], D(X^nP)=X^nD(P)+PD(X^n)$$

Soit $P\in\mathbb{K}[X]$. Soient :

$$u_3 : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ Q & \longmapsto & D(PQ) \end{cases} \qquad \text{et} \qquad u_4 : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & QD(P)+PD(Q) \end{cases}$$ □

On vient donc de prouver que u_3 et u_4 coïncident sur la base canonique $(X^n)_{n\in\mathbb{N}}$ donc sont égales, ce qui est le résultat voulu.

Remarque : Passons maintenant aux dérivées successives. Précisons que, si $k\in\mathbb{N}$, alors $P^{(k)}$ est le polynôme obtenu en dérivant k fois P donc en appliquant k fois l'opérateur de dérivation D, si bien que $P^{(k)}=D^k(P)$.

Proposition (Formule de Taylor pour les polynômes). Soit $P \in \mathbb{K}[X]$ et soit $\alpha \in \mathbb{K}$. Alors

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha) \times (X-\alpha)^k}{k!}$$

En particulier, si P est de degré n, alors

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

Démonstration. Avec la notation D, il suffit donc de prouver que

$$P = \sum_{k=0}^{+\infty} \frac{D^k(P)(\alpha) \times (X-\alpha)^k}{k!}$$

Notons

$$u : \begin{cases} \mathbb{K}[X] & \longrightarrow \quad \mathbb{K}[X] \\ P & \longmapsto \displaystyle\sum_{k=0}^{+\infty} \frac{D^k(P)(\alpha) \times (X-\alpha)^k}{k!} \end{cases}$$

Alors u est linéaire puisque D l'est. Il suffit donc de prouver que u et $\mathrm{Id}_{\mathbb{K}[X]}$ coïncident sur une base pour conclure. Prouvons que la famille $((X-\alpha)^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$: c'est une famille échelonnée en degré donc une famille libre, il suffit donc de prouver qu'elle est génératrice. Soit $P \in \mathbb{K}[X]$. Il suffit de « translater » : $(X^n)_{n\in\mathbb{N}}$ étant génératrice, le polynôme $Q = P(X+\alpha)$ est CL des X^n donc il existe $(a_n)_{n\in\mathbb{N}}$ famille presque nulle telle que

$$Q = \sum_{n=0}^{+\infty} a_n X^n$$

Par conséquent :

$$Q \circ (X-\alpha) = \sum_{n=0}^{+\infty} a_n (X-\alpha)^n$$

c'est-à-dire que

$$P(X) = \sum_{n=0}^{+\infty} a_n (X-\alpha)^n$$

La famille est génératrice : c'est bien une base. Par conséquent, il suffit de prouver que u et $\mathrm{Id}_{\mathbb{K}[X]}$ coïncident sur cette base pour conclure. Soit donc $n \in \mathbb{N}$. Pour tout $k \in \mathbb{N}$:

- $D^k((X-\alpha)^n) = n(n-1)\cdots(n-k+1)(X-\alpha)^{n-k}$ si $k \leqslant n-1$ et en particulier sa valeur en α est nulle.
- $D^n((X-\alpha)^n) = n!$.
- $D^k((X-\alpha)^n) = 0$ si $k > n$.

En conclusion, il n'y a qu'un terme non nul dans la somme définissant $u((X-\alpha)^n)$, qui vaut

$$\frac{n! \times (X-\alpha)^n}{n!} = (X-\alpha)^n$$ □

En d'autres termes, u et $\mathrm{Id}_{\mathbb{K}[X]}$ coïncident sur la base $((X-\alpha)^n)_{n\in\mathbb{N}}$ (qui n'est pas la base canonique !) donc sont égales.

Théorème. Soit $n \in \mathbb{N}^*$. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P de multiplicité n si et seulement si

$$P(\alpha) = P'(\alpha) = \cdots = P^{(n-1)}(\alpha) = 0 \qquad \text{et} \qquad P^{(n)}(\alpha) \neq 0.$$

En particulier, α est racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

La multiplicité d'une racine α est donc l'ordre de la première dérivée non nulle en α.

Démonstration. Notons $d = \deg(P)$. D'après le théorème de division euclidienne, il existe Q et R appartenant à $\mathbb{K}[X]$ uniques tels que $P = Q_1(X-\alpha)^n + R_1$ avec $\deg(R_1) < n$. Or, d'après la formule de Taylor pour les polynômes,

$$\begin{aligned} P &= \sum_{k=0}^{d} \frac{P^{(k)}(\alpha)}{k!}(X-a)^k \\ &= \underbrace{\sum_{k=0}^{n-1} \frac{P^{(k)}(\alpha)}{k!}(X-a)^k}_{\text{de degré} \leqslant n-1 < n} + (X-\alpha)^n \left(\sum_{k=n}^{d} \frac{P^{(k)}(\alpha)}{k!}(X-a)^{k-n} \right). \end{aligned}$$

On a une écriture de P sous la forme $A(X-\alpha)^n + B$ avec $\deg(B) < n$. Par unicité de l'écriture de la division euclidienne, $R_1 = B$ et $Q_1 = A$, c'est-à-dire :

$$R_1 = \sum_{k=0}^{n-1} \frac{P^{(k)}(\alpha)}{k!}(X-a)^k \qquad \text{et} \qquad Q = \sum_{k=n}^{d} \frac{P^{(k)}(\alpha)}{k!}(X-a)^{k-n}.$$

De même, le reste dans la division euclidienne de P par $(X-\alpha)^{n+1}$ est

$$R_2 = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-a)^k.$$

- Supposons que α soit racine de P de multiplicité n. Alors $(X-\alpha)^n$ divise P, et $(X-\alpha)^{n+1}$ ne divise pas P, c'est-à-dire que $R_1 = 0$ et $R_2 \neq 0$. Or $\left((X-\alpha)^k\right)_{0 \leqslant k \leqslant n-1}$ est une famille échelonnée en degré donc une famille libre. Le fait que $R_1 = 0$ entraîne que $P^{(k)}(\alpha) = 0$ pour tout $k \in [\![0\,;\, n-1]\!]$. Par conséquent, tous les termes d'indice k allant de 0 à $n-1$ de la somme de R_2 sont nuls, si bien que $R_2 = \dfrac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n$. Comme $R_2 \neq 0$, on a $P^{(n)}(\alpha) \neq 0$.
- Réciproquement, supposons que $P(\alpha) = \cdots = P^{(n-1)}(\alpha) = 0 \neq P^{(n)}(\alpha)$. Il découle alors immédiatement des expressions de R_1 et R_2 que $R_1 = 0$ et $R_2 \neq 0$ donc $(X-\alpha)^n$ divise P mais $(X-\alpha)^{n+1}$ ne divise pas P, ce qui permet de conclure. □

V Projecteurs et symétries

V.1 Projecteurs

V.1.a Définition

Définition. Soient E_1 et E_2 deux sev de E supplémentaires. Par conséquent, pour tout $x \in E$, il existe $x_1 \in E_1$ et $x_2 \in E_2$ uniques tels que $x = x_1 + x_2$. L'application

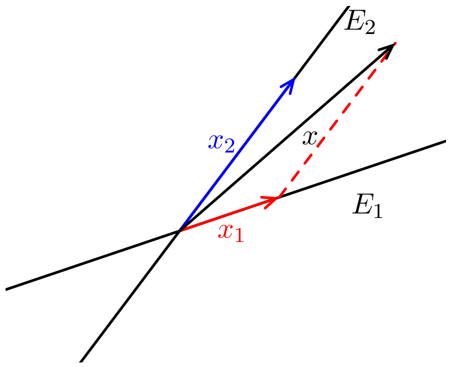
$$p : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & x_1 \end{array} \right.$$

est appelée projecteur sur E_1 parallèlement à E_2.

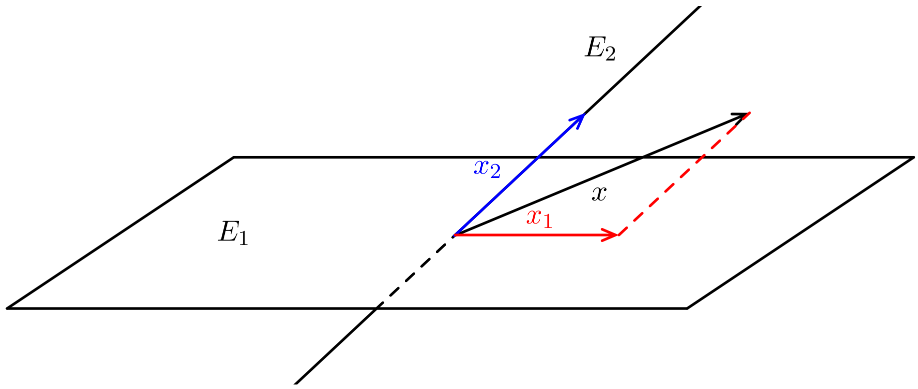
Pour faire simple : la projection (on parle indifféremment de projecteur ou de projection), c'est la « partie du vecteur qui appartient à E_1 ». Il faut donc au préalable avoir écrit x sous cette forme : voir quelques exemples ci-dessous.

Exemples : Ci-dessous, on a à chaque fois deux sous-espaces vectoriels supplémentaires E_1 et E_2, et on a $p(x) = x_1$.

- Dans $\mathbb{R}^2$:



- Dans $\mathbb{R}^3$:



Remarques :

- E_1 et E_2 n'ont aucune raison d'être orthogonaux (d'ailleurs, on ne sait pas encore définir deux sev orthogonaux, cf. chapitre 34). Ainsi, quand on fera un dessin, on dessinera des sev en position générale, comme ci-dessus.
- E_2 est parfois appelée la direction de p : c'est intuitif, quand on projette, on le fait parallèlement à E_2 donc on suit la « direction » E_2.

Avec les mains : une projection n'est rien d'autre que l'application « ombre » lorsque le soleil est dans la direction E_1. C'est une application linéaire (un objet deux fois plus grand aura une ombre deux fois plus grande), le noyau est E_1 (un élément n'a pas d'ombre lorsqu'il est parallèle aux rayons du soleil), l'image est E_2 (on peut avoir des ombres de tout type) et $p^2 = p$ (l'ombre de l'ombre, c'est l'ombre). Tout est intuitif !

Proposition. Avec les notations précédentes :

- $p \in \mathscr{L}(E)$.
- $\ker(p) = E_2$.
- $\mathrm{Im}(p) = E_1$.
- $p^2 = p$.

Démonstration.

- Soient $(x, y) \in E^2, \lambda \in \mathbb{K}$. Il existe $(x_1, y_1) \in {E_1}^2$ et $(x_2, y_2) \in {E_2}^2$ uniques tels que

$$x = x_1 + x_2 \qquad \text{et} \qquad y = y_1 + y_2$$

Ainsi, $\lambda x = \underbrace{\lambda x_1}_{\in E_1} + \underbrace{\lambda x_2}_{\in E_2}$, d'où :

$$\begin{aligned} p(\lambda x) &= \lambda x_1 \\ &= \lambda p(x) \end{aligned}$$

L'égalité $p(x+y) = p(x) + p(y)$ se démontre de la même façon : p est bien linéaire, et $p : E \to E$ donc p est bien linéaire.

- Supposons que $x \in \ker(p)$. Alors $p(x) = 0$ donc $x_1 = 0$ (on rappelle que $p(x) = x_1$), si bien que $x = 0 + x_2 \in E_2$: $\ker(p) \subset E_2$. Réciproquement, supposons que $x \in E_2$. Alors

$$x = \underbrace{0}_{\in E_1} + \underbrace{x_2}_{\in E_2}$$

□

donc $p(x) = 0$ ie $x \in \ker(p)$. D'où l'inclusion réciproque, d'où l'égalité.

- Pour l'image : exo.
- Enfin, $p(x) = x_1 \in E_1$ donc

$$p(x) = \underbrace{p(x)}_{\in E_1} + \underbrace{0}_{\in E_2}$$

Ainsi, $p(p(x)) = p(x)$ ie $p^2(x) = p(x)$: $p^2 = p$.

Un dernier résultat pour la route :

Proposition. Avec les notations précédentes : $\forall x \in E_1, p(x) = x$. En d'autres termes, p laisse tous les éléments de E_1 invariants.

Démonstration. Puisque $x \in E_1$, alors $x = \underbrace{x}_{\in E_1} + \underbrace{0}_{\in E_2}$ ce qui permet de conclure.

Remarque : Ce résultat est assez utile en pratique : par exemple, si p et q sont deux projecteurs sur E_1, alors $p \circ q = q$ et $q \circ p = p$. En effet, pour tout x, $q(x) \in E_1$ donc $p(q(x)) = q(x)$ et idem pour l'autre : cf. exercice 39 par exemple.

V.1.b Caractérisation pratique

Théorème. Soit $p \in \mathscr{L}(E)$ tel que $p^2 = p$. Alors p est un projecteur. Plus précisément, p est le projecteur sur $\mathrm{Im}(p)$ parallèlement à $\ker(p)$.

Démonstration. On veut montrer que p est un projecteur ie qu'il existe E_1 et E_2 supplémentaires tels que si x s'écrit

$$x = \underbrace{x_1}_{\in E_1} + \underbrace{x_2}_{\in E_2}$$

alors $p(x) = x_1$. On sait d'après la proposition précédente que si E_1 et E_2 conviennent alors $E_1 = \mathrm{Im}(p)$ et $E_2 = \ker(p)$. On veut donc montrer que $\ker(p)$ et $\mathrm{Im}(p)$ sont supplémentaires et que p est la projection sur $\mathrm{Im}(p)$ parallèlement à $\ker(p)$. Montrons donc que $E = \mathrm{Im}(p) \oplus \ker(p)$. Soit $x \in E$. Montrons qu'il existe $x_1 \in \mathrm{Im}(p)$ et $x_2 \in \ker(p)$ uniques tels que $x = x_1 + x_2$.

Analyse : Si x_1 et x_2 conviennent,

$$\begin{aligned} p(x) &= p(x_1 + x_2) \\ &= p(x_1) + p(x_2) \qquad (p \text{ est linéaire}) \\ &= p(x_1) \qquad (\text{car } x_2 \in \ker(p)) \end{aligned}$$

Or, $x_1 \in \mathrm{Im}(p)$: il existe $y_1 \in E$ tel que $x_1 = p(y_1)$ donc

$$\begin{aligned} p(x) &= p(p(y_1)) \\ &= p^2(y_1) \\ &= p(y_1) \qquad \text{(car } p^2 = p\text{)} \\ &= x_1 \end{aligned}$$

En d'autres termes, $x_1 = p(x)$ et

$$\begin{aligned} x_2 &= x - x_1 \\ &= x - p(x) \end{aligned}$$

Synthèse : Soient $x_1 = p(x)$ et $x_2 = x - p(x)$. Montrons que :

- $x_1 \in \text{Im}(p)$: OK.
- $x_1 + x_2 = x$: OK.
- $x_2 \in \ker(p)$.

Or :

$$\begin{aligned} p(x_2) &= p(x - p(x)) \\ &= p(x) - p(p(x)) \qquad \text{(car } p \text{ est linéaire)} \\ &= 0 \qquad \text{(car } p^2 = p\text{)} \end{aligned}$$

On a bien $p_2 \in \ker(p)$: $\text{Im}(p)$ et $\ker(p)$ sont bien supplémentaires. De plus, si $x \in E$ alors

$$x = \underbrace{p(x)}_{\in \text{Im}(p)} + \underbrace{(x - p(x))}_{\in \ker(p)}$$

□

Ci-dessus, $p(x)$ joue donc le rôle de x_1 et $x - p(x)$ celui de x_2. En conclusion, on a $p(x) = x_1$: p est bien le projecteur sur $\text{Im}(p)$ parallèlement à $\ker(p)$.

Corollaire. Soit $p \in \mathscr{L}(E)$. p est un projecteur si et seulement si $p^2 = p$, et alors :

- $\ker(p)$ et $\text{Im}(p)$ sont supplémentaires.
- p est le projecteur sur $\text{Im}(p)$ parallèlement à $\ker(p)$.

Par conséquent, la première chose à faire quand on veut prouver qu'une application p est un projecteur est de prouver que $p \circ p = p$ (et aussi que p est linéaire si cela n'est pas supposé par l'énoncé).

V.2 Symétries

Les résultats de ce paragraphe ne sont pas valables sur un corps quelconque, mais uniquement sur un corps de caractéristique différente de 2 (par exemple, cela ne marche pas sur $\mathbb{Z}/2\mathbb{Z}$). Mais bon... puisque le programme se limite au cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, cette remarque est violemment hors programme et ne nous servira à rien en pratique donc, chut, je n'ai rien dit.

V.2.a Définition

Définition. Soient E_1 et E_2 deux sev de E supplémentaires. Par conséquent, pour tout $x \in E$, il existe $x_1 \in E_1$ et $x_2 \in E_2$ uniques tels que $x = x_1 + x_2$. L'application

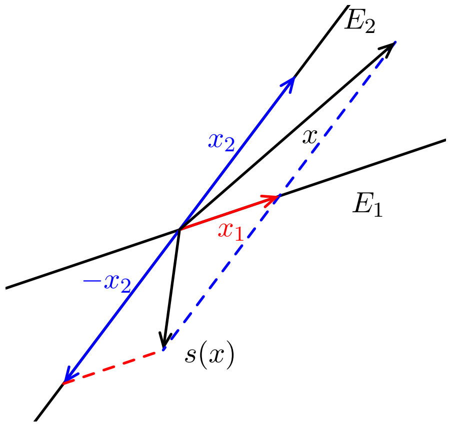
$$s:\left\{\begin{array}{ccc} E & \to & E \\ & & \\ x & \mapsto & x_1 - x_2 \end{array}\right.$$

est appelée symétrie par rapport à E_1 parallèlement à E_2.

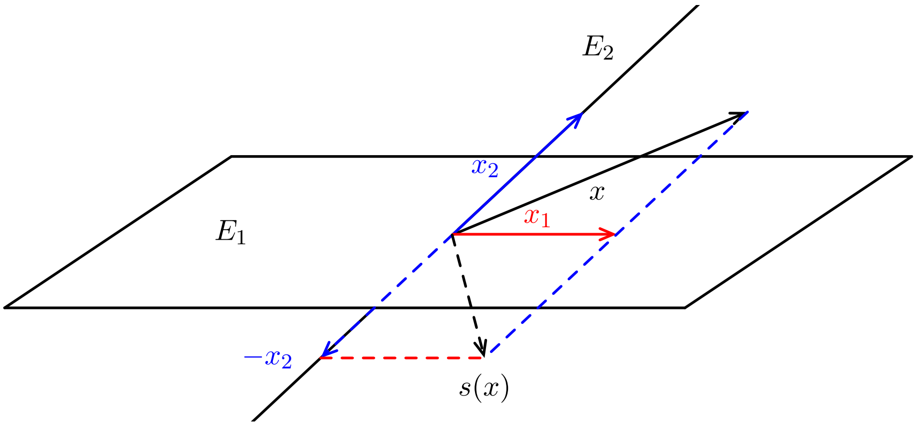
Remarque : Comme pour un projecteur, E_2 est parfois appelé la direction de s.

Exemples : Ci-dessous, on a à chaque fois deux sous-espaces vectoriels supplémentaires E_1 et E_2, et on a $s(x) = x_1 - x_2$.

- Dans $\mathbb{R}^2$:



- Dans $\mathbb{R}^3$:



On peut remarquer (ce qui est contraire à l'intuition mais c'est parce qu'on a l'habitude des projections orthogonales) que x et $s(x)$ n'ont pas « la même longueur » : mais qu'est-ce que la longueur dans un espace vectoriel ? Qu'est-ce que la longueur d'une suite, d'une fonction, d'une matrice donnée ? Réponse en deuxième année ! Un moyen simple de s'en rendre compte est de voir que $x_1 + x_2$ et $x_1 - x_2$ sont les vecteurs formés par les deux diagonales du parallélogramme formé par x_1 et x_2 (même si on représente en général $x_1 - x_2$ comme un vecteur partant de l'origine, comme d'habitude.

Proposition. Avec les notations précédentes :

- $s \in \mathscr{L}(E)$.
- $\ker(s) = \{0\}$.
- $\text{Im}(s) = E$.
- $s^2 = \text{Id}_E$.

Démonstration.
- La linéarité de s est analogue à la linéarité de p dans le paragraphe V.1.a.
- Supposons que $x \in \ker(s)$. Alors $s(x) = 0$ donc $x_1 - x_2 = 0$ donc $x_1 = x_2$ et puisque $x_1 \in E_1$ et $x_2 \in E_2$, alors $x_1 = x_2 \in E_1 \cap E_2 = \{0\}$ car les deux espaces sont supplémentaires. On en déduit que $x = 0$: $\ker(s) = \{0\}$.
- Pour l'image : exo.
- Le fait que $s(s(x)) = x$ se démontre de façon analogue à l'égalité $p(p(x)) = p(x)$ du paragraphe V.1.a.

En d'autres termes : une symétrie est injective, ce qui est intuitif, car deux vecteurs ont même image par une symétrie si et seulement s'ils sont égaux.

Corollaire. Une symétrie est une bijection et est sa propre bijection réciproque.

DÉMONSTRATION. Soit $s : E \to E$ une symétrie. $s \circ s = s \circ s = \mathrm{Id}_E$ donc s est bijective et $s^{-1} = s$.

Remarque : L'image et le noyau n'ont que peu d'intérêt pour une symétrie. Les espaces suivants sont plus importants puisqu'ils dirigent en quelque sorte la symétrie.

Proposition/Définition. Soit $s : E \to E$ une symétrie. Notons

$$A_1 = \{x \in E \,|\, s(x) = x\} \qquad \text{et} \qquad A_2 = \{x \in E \,|\, s(x) = -x\}$$

Alors A_1 et A_2 sont deux sous-espaces vectoriels supplémentaires de E, et s est la symétrie par rapport à A_1 parallèlement à A_2.

Cela se voit bien sur les dessins ci-dessus : les éléments de E_1 sont exactement ceux laissés invariants par s, et les éléments de E_2 sont exactement ceux changés en leur opposé : une symétrie n'est pas par rapport à son noyau parallèlement à son image (comme un projecteur) mais par rapport à son ensemble des invariants parallèlement à l'ensemble des éléments qu'elle envoie sur leur opposé.

DÉMONSTRATION. Tout d'abord, notons E_1 et E_2 les deux sous-espaces vectoriels supplémentaires définissant s, c'est-à-dire tels que s soit la symétrie par rapport à E_1 parallèlement à E_2. Il suffit de prouver que $A_1 = E_1$ et $A_2 = E_2$ (même si on pourrait prouver certains résultats directement : par exemple, A_1 est un sev de E car est le noyau de $s - \mathrm{Id}_E$). Soit $x = x_1 + x_2 \in E$ (où, évidemment, $x_1 \in E_1$ et $x_2 \in E_2$). Alors $s(x) = x_1 - x_2$. On en déduit deux choses :

- $x \in A_1 \iff s(x) = x \iff x_2 = 0 \iff x \in E_1$ donc $A_1 = E_1$.
- $A_2 = E_2$ de la même façon.

V.2.b Caractérisation pratique

Théorème. Soit $p \in \mathscr{L}(E)$ tel que $s^2 = \mathrm{Id}_E$. Alors s est une symétrie. Plus précisément, en reprenant les notations ci-dessus, s est la symétrie par rapport à A_1 parallèlement à A_2.

DÉMONSTRATION. On veut montrer que s est une symétrie ie qu'il existe E_1 et E_2 supplémentaires tels que si x s'écrit

$$x = \underbrace{x_1}_{\in E_1} + \underbrace{x_2}_{\in E_2}$$

alors $s(x) = x_1 - x_2$. On sait d'après la proposition précédente que si E_1 et E_2 conviennent alors $E_1 = A_1$ et $E_2 = A_2$. On veut donc montrer que A_1 et A_2 sont supplémentaires Montrons donc que $E = A_1 \oplus A_2$. Tout d'abord, $A_1 = \ker(f - \mathrm{Id}_E)$ donc est un sev de E, et idem pour A_2.

Attention, la proposition ci-dessus n'est plus valide puisqu'on veut prouver que s est une symétrie : on ne sait donc pas encore que A_1 et A_2 sont supplémentaires. et que s est la symétrie par rapport à E_1 parallèlement à E_2.

Soit $x \in E$. Montrons qu'il existe $x_1 \in A_1$ et $x_2 \in A_2$ uniques tels que $x = x_1 + x_2$.

Analyse : Si x_1 et x_2 conviennent,

$$\begin{aligned} s(x) &= s(x_1 + x_2) \\ &= s(x_1) + s(x_2) \qquad (p \text{ est linéaire}) \\ &= x_1 - x_2 \end{aligned}$$

Rappelons que $x = x_1 + x_2$ si bien que

$$x_1 = \frac{1}{2}(x + s(x)) \qquad \text{et} \qquad x_2 = \frac{1}{2}(x - s(x))$$

Synthèse : Soient

$$x_1 = \frac{1}{2}(x + s(x)) \qquad \text{et} \qquad x_2 = \frac{1}{2}(x - s(x))$$

Montrons que :

- $x_1 \in A_1$.
- $x_2 = A_2$.
- $x = x_1 + x_2$: OK.

Or :

$$\begin{aligned} s(x_1) &= \frac{1}{2}(s(x) + s(s(x))) \quad \text{(car } p \text{ est linéaire)} \\ &= \frac{1}{2}(x + s(x)) \qquad\qquad \text{(car } s^2 = \mathrm{Id}_E) \end{aligned}$$

On a bien $s(x_1) = x_1$. De même, $s(x_2) = -x_2$: A_1 et A_2 sont bien supplémentaires. De plus, si $x \in E$ alors

$$x = \underbrace{\frac{1}{2}(x + s(x))}_{\in A_1} + \underbrace{\frac{1}{2}(x - s(x))}_{\in A_2}$$

□

Ci-dessus, le premier terme joue donc le rôle de x_1 et le deuxième celui de x_2. En conclusion, on a $s(x) = x_1 - x_2$: s est bien la symétrie par rapport à A_1 parallèlement à A_2.

Corollaire. Soit $s \in \mathscr{L}(E)$. p est une symétrie si et seulement si $s^2 = \mathrm{Id}_E$, et alors :

- A_1 et A_2 sont supplémentaires.
- s est la la symétrie par rapport à A_1 parallèlement à A_2.

Par conséquent, la première chose à faire quand on veut prouver qu'une application s est une symétrie est de prouver que $s \circ s = \mathrm{Id}_E$ (et aussi que s est linéaire si cela n'est pas supposé par l'énoncé).

VI Marches à suivre et exemples

VI.1 Pour donner une base d'un noyau ou d'une image

Il est très fréquent qu'on demande une base d'un noyau ou d'une image. La méthode est toujours la même. Pour l'image :

- On se rappelle que l'image d'une famille génératrice est une famille génératrice de l'image. Par conséquent, si G est une famille génératrice de E, alors $u(G)$ est génératrice de $\mathrm{Im}(u)$.
- On retire les vecteur superflus : rappelons que si un vecteur est CL des autres, on peut le retirer et on engendre encore le même espace (cf. chapitre 29).
- Lorsque les vecteurs restants sont libres, on a une famille libre qui est encore génératrice (car, à chaque étape, l'espace engendré est le même) donc une base.

Pour le noyau :

- On part de l'équation $u(x) = 0$, on arrive à une ou plusieurs équations et on met le noyau sous forme de Vect de la même manière que dans le chapitre 28. On obtient donc une famille génératrice du noyau.
- On effectue les mêmes deux dernières étapes que pour l'image (enlever les vecteurs superflus jusqu'à obtenir une famille libre).

Exemple : Soit

$$u\colon \begin{cases} \mathbb{K}^3 & \longrightarrow & \mathbb{K}^3 \\ (x,y,z) & \longmapsto & (2x - y + 3z, x - 2y, -x - 2y - 4z) \end{cases}$$

Il s'agit d'un endomorphisme de $\mathbb{R}^3$. ⇝ Exercice.

Donnons une base du noyau et de l'image de u. Commençons par l'image. Puisque la base canonique de $\mathbb{K}^3$ (e_1, e_2, e_3) engendre $\mathbb{K}^3$, alors $u(e_1), u(e_2)$ et $u(e_3)$ forment une famille génératrice de $\mathrm{Im}(u)$:

$$\begin{aligned}\mathrm{Im}(u) &= \mathrm{Vect}\Big(u(1,0,0), u(0,1,0), u(0,0,1)\Big)\\ &= \mathrm{Vect}\Big(\underbrace{(2,1,-1)}_{=u(e_1)}, \underbrace{(-1,-2,-2)}_{=u(e_2)}, \underbrace{(3,0,-4)}_{=u(e_3)}\Big).\end{aligned}$$

Cherchons si ces trois vecteurs sont libres. Soit $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{K}^3$.

$$\begin{aligned}\lambda_1 u(e_1) + \lambda_2 u(e_2) + \lambda_3 u(e_3) = 0 \quad &\iff \quad \begin{cases} 2\lambda_1 - \lambda_2 + 3\lambda_3 = 0\\ \lambda_1 - 2\lambda_2 = 0\\ -\lambda_1 - 2\lambda_2 - 4\lambda_3 = 0\end{cases}\\
&\iff \quad \begin{cases} 2\lambda_1 - \lambda_2 + 3\lambda_3 = 0\\ - 3\lambda_2 - 3\lambda_3 = 0\end{cases}\\
&\iff \quad \begin{cases} 2\lambda_1 = \lambda_2 - 3\lambda_3\\ \lambda_3 = -\lambda_2\end{cases}\\
&\iff \quad \begin{cases} \lambda_1 = 2\lambda_2\\ \lambda_3 = -\lambda_2\end{cases}\end{aligned}$$

$\lambda_1 = 2, \lambda_2 = 1$ et $\lambda_3 = -1$ conviennent : la famille est liée. Plus fort : $u(e_3) = 2u(e_1) + u(e_2)$ donc $u(e_3)$ est CL de $u(e_1)$ et $u(e_2)$ donc $\mathrm{Im}(u) = \mathrm{Vect}(u(e_1), u(e_2))$. On se demande à présent si $u(e_1)$ et $u(e_2)$ sont libres, ce qui est immédiat puisqu'ils ne sont pas colinéaires (ce critère n'est valable que pour deux vecteurs, cf. chapitre 28). Par conséquent, $u(e_1) = (2,1,-1)$ et $u(e_2) = (-1,-2,-2)$ forment une base de $\mathrm{Im}(u)$.

Rappelons que la solution nulle $\lambda_1 = \lambda_2 = \lambda_3 = 0$ convient toujours : la famille est libre lorsque c'est la seule.

Les calculs sont les mêmes ! C'est normal : $\lambda_1 u(e_1) + \lambda_2 u(e_2) + \lambda_3 u(e_3) = 0$ si et seulement si $\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 \in \ker(u)$.

Donnons à présent une base du noyau.
Déterminons son noyau. On se donne $(x, y, z) \in \mathbb{K}^3$. On a :

$$\begin{aligned}(x,y,z) \in \mathrm{Ker}(u) \quad &\iff \quad u(x,y,z) = (0,0,0)\\
&\iff \quad (2x - y + 3z, x - 2y, -x - 2y - 4z) = (0,0,0)\\
&\iff \quad \begin{cases} 2x - y + 3z = 0\\ x - 2y = 0\\ -x - 2y - 4z = 0\end{cases}\\
&\iff \quad \begin{cases} 2x - y + 3z = 0\\ - 3y - 3z = 0\end{cases}\\
&\iff \quad \begin{cases} 2x = y - 3z\\ z = -y\end{cases}\\
&\iff \quad \begin{cases} x = 2y\\ z = -y\end{cases}\end{aligned}$$

Nous obtenons donc que $\mathrm{Ker}(u) = \{(y(2,1,-1) \,|\, y \in \mathbb{K}\} = \mathrm{Vect}\big((2,1,-1)\big)$. $(2,1,-1)$ est donc une famille génératrice du noyau, et c'est aussi une famille libre puisque c'est une famille à un élément qui est non nul : c'est donc une base.

Remarque : On a un élément dans la base du noyau et deux éléments dans la base de l'image. De plus, u est définie sur $\mathbb{K}^3$ et $3 = 1 + 2$. Ce n'est pas un hasard : c'est un cas particulier du théorème du rang, cf. chapitre 30.

VI.2 Pour expliciter un projecteur ou une symétrie

La méthode est toujours la même pour donner l'expression explicite d'un projecteur ou d'une symétrie :

- On écrit chaque élément de E comme somme d'un élément $x_1 \in E_1$ et d'un élément $x_2 \in E_2$. On raisonne en général par analyse-synthèse (dans des espaces « compliqués ») ou par équivalences (dans des espaces « simples ») comme ci-dessus et comme dans le chapitre 28.
- Si on cherche le projecteur sur E_1 parallèlement à E_2, on renvoie x_1 (le premier vecteur), sinon on renvoie $x_1 - x_2$ (le premier moins le deuxième).

Exemples :

- Soient $E_1 = \text{Vect}((-1,0,1))$ et $E_2 = \{(x,y,z) \in \mathbb{K}^3 \,|\, x-y-z=0\}$. Montrons que $\mathbb{K}^3 = E_1 \oplus E_2$. Raisonnons par analyse synthèse. Plus précisément, soit $x=(a,b,c) \in \mathbb{K}^3$. Montrons par analyse-synthèse qu'il existe $x_1 \in E_1$ et $x_2 \in E_2$ uniques tels que $x = x_1 + x_2$.

  ⋆ **Analyse :** Si $x_1 = (a_1, b_1, c_1)$ et $x_2 = (a_2, b_2, c_2)$ conviennent. Puisque $x_1 \in E_1$, il existe $\lambda \in \mathbb{K}$ tel que $x_1 = \lambda(-1,0,1)$ donc $a_1 = -\lambda, b_1 = 0$ et $c_1 = \lambda$. De plus, $x_2 \in E_2$ donc $a_2 - b_2 - c_2 = 0$ donc $a_2 = b_2 + c_2$. On en déduit donc que

  $$(a,b,c) = (-\lambda, 0, \lambda) + (b_2 + c_2, b_2, c_2)$$

  On arrive alors au système suivant (d'inconnues λ, b_2, c_2) :

  $$\left\{\begin{array}{rcccccl} -\lambda & + & b_2 & + & c_2 & = & a \\ & & b_2 & & & = & b \\ \lambda & & & + & c_2 & = & c \end{array}\right.$$

  $$\iff \left\{\begin{array}{rcccl} -\lambda & & + \; c_2 & = & a-b \\ & b_2 & & = & b \\ \lambda & & + \; c_2 & = & c \end{array}\right.$$

  Finalement, on trouve :

  $$\lambda = \frac{-a+b+c}{2} \qquad \text{et} \qquad c_2 = \frac{a-b+c}{2}$$

  si bien que

  $$x_1 = \left(\frac{a-b-c}{2}, 0, \frac{-a+b+c}{2}\right) \qquad \text{et} \qquad x_2 = \left(\frac{a+b+c}{2}, b, \frac{a-b+c}{2}\right)$$

  ⋆ **Synthèse :** Soient

  $$x_1 = \left(\frac{a-b-c}{2}, 0, \frac{-a+b+c}{2}\right) \qquad \text{et} \qquad x_2 = \left(\frac{a+b+c}{2}, b, \frac{a-b+c}{2}\right)$$

  Alors $x_1 \in E_1$, $x_2 \in E_2$ puisque

  $$\begin{aligned} \frac{a+b+c}{2} - b - \frac{a-b+c}{2} &= \frac{a+b+c-2b-a+b-c}{2} \\ &= 0 \end{aligned}$$

  et $x_1 + x_2 = (a,b,c) = x$: on a prouvé que tout élément de $\mathbb{K}^3$ s'écrit de façon unique comme somme d'un élément de E_1 et d'un élément de E_2, c'est-à-dire que $\mathbb{K}^3 = E_1 \oplus E_2$. Enfin, la projection sur E_1 parallèlement à E_2 et la symétrie par rapport à E_1 parallèlement à E_2 sont respectivement :

  $$p \colon \left\{\begin{array}{ccc} \mathbb{K}^3 & \longrightarrow & \mathbb{K}^3 \\ (a,b,c) & \longmapsto & \left(\dfrac{a-b-c}{2}, 0, \dfrac{-a+b+c}{2}\right) \end{array}\right.$$

et

$$s\colon \begin{cases} \mathbb{K}^3 & \longrightarrow & \mathbb{K}^3 \\ (a,b,c) & \longmapsto & \left(\dfrac{a-b-c}{2}, 0, \dfrac{-a+b+c}{2}\right) - \left(\dfrac{a+b+c}{2}, b, \dfrac{a-b+c}{2}\right) = (-b-c, -b, -a+b) \end{cases}$$

- On a prouvé que $\mathscr{M}_n(\mathbb{K}) = S_n(\mathbb{K}) \oplus A_n(\mathbb{K})$ et que, pour tout $M \in \mathscr{M}_n(\mathbb{K})$,

$$M = \underbrace{\frac{1}{2}(M + M^\top)}_{\in S_n(\mathbb{K})} + \underbrace{\frac{1}{2}(M - M^\top)}_{\in A_n(\mathbb{K})}$$

  Par conséquent, la fonction $M \mapsto \dfrac{1}{2}(M + M^\top)$ est le projecteur sur $S_n(\mathbb{K})$ parallèlement à $A_n(\mathbb{K})$.

- De même, la fonction

$$p\colon \begin{cases} \mathbb{R}^\mathbb{R} & \longrightarrow & \mathbb{R}^\mathbb{R} \\ f & \longmapsto & x \mapsto \dfrac{1}{2}(f(x) + f(-x)) \end{cases}$$

  est la projection sur l'ensemble des fonctions paires parallèlement à l'ensemble des fonctions impaires. Par exemple, la fonction ch n'est rien d'autre que la partie paire de l'exponentielle !

Remarque : Parfois, on demande d'expliciter les éléments caractéristiques d'un projecteur ou d'une symétrie (cf. par exemple l'exercice 35). Les deux situations sont différentes :

- pour un projecteur, on demande son noyau et son image. Rappelons qu'un projecteur projette sur son noyau parallèlement à son image.
- pour une symétrie, on demande $A_1 = \{x \,|\, s(x) = x\}$ et $A_2 = \{x \,|\, s(x) = -x\}$. Rappelons qu'une symétrie projette par rapport à A_1 parallèlement à A_2.

Ne pas confondre les deux !