Espaces vectoriels

Marc SAGE

26 janvier 2009

Table des matières

On abrégera dans la suite « (sous-)ev » en « $(s)ev$ ».

1 Quelques contre-exemples

1. *Trouver un endomorphisme sur un ev qui soit injectif non surjectif, puis surjectif non injectif.*
2. *Trouver un ev E tel que $\forall n \geq 3$ on puisse trouver n sous-ev $F_1, ..., F_n$ deux à deux en somme directe mais pas tous en somme directe.*
3. *Donner des exemples d'endomorphismes dont le noyau et l'image ne sont pas en somme directe.*
4. *Exhiber un endomorphisme dont le noyau et l'image sont en somme directe mais qui n'est pas un projecteur*[1]
5. *Montrer qu'un produit de nilpotents n'est pas forcément nilpotent.*

Solution proposée.

1. D'après le cours sur la dimension finie, il faut que E soit de dimension infinie. On considère par exemple l'ev $E^{\mathbb{N}}$ des suites dans un ev E où les applications « décalage » vers la gauche γ et vers la droite δ définies par
$$\begin{cases} \gamma : (u_0, u_1, ...) \mapsto (u_1, u_2, ...) \\ \delta : (u_0, u_1, ...) \mapsto (0, u_0, u_1, ...) \end{cases}$$
vérifient $\begin{cases} \gamma \text{ surjective non injective} \\ \delta \text{ injective non surjective} \end{cases}$.
2. Prendre $\mathbb{R}^2$ et n droites distinctes.
3. Il suffit d'avoir l'une des inclusions $\begin{cases} \{0\} \subsetneq \operatorname{Ker} u \subset \operatorname{Im} u \\ \{0\} \subsetneq \operatorname{Im} u \subset \operatorname{Ker} u \end{cases}$. La première inclusion peut être obtenue pour des endomorphismes surjectifs non injectifs, par exemple l'opérateur dérivation dans $\mathbb{R}[X]$; la seconde inclusion signifie que $u^2 = 0$ et $u \neq 0$, par exemple dans $\mathbb{R}^2$ l'application $u : (x, y) \longmapsto (y, 0)$.

   Pour un autre exemple, considérer un endomorphisme u nilpotent d'indice $p \geq 2$ et $x \notin \operatorname{Ker} u^{p-1}$: alors le vecteur $u^{p-1}(x)$ est non nul et tombe dans $\operatorname{Ker} u \cap \operatorname{Im} u$.
4. Soit A et B deux sev supplémentaires. On remarque que, selon la décomposition $E = A \oplus B$, tout endomorphisme de la forme $\varphi \oplus 0$ où $\varphi \in GL(A)$ est d'image A et de noyau B. Pour que $\varphi \oplus 0$ ne soit pas un multiple scalaire d'un projecteur, il faut et suffit que φ n'en soit pas un ; le seul projecteur inversible étant l'identité, n'importe quel $\varphi \in GL(A) \backslash K \operatorname{Id}_A$ fera l'affaire (ce qui impose bien sûr $K \operatorname{Id}_A \subsetneq GL(A)$, *i. e.* $\dim A > 1$).
5. Considérer dans K^n les endomorphismes « tapis roulant » :
$$\begin{cases} (a_1, ..., a_n) \mapsto (0, a_1, ..., a_{n-1}) \text{ (tapis roulant vers la droite)} \\ (a_1, ..., a_n) \mapsto (a_2, ..., a_n, 0) \text{ (tapis roulant vers la gauche)} \end{cases}.$$

2 Sur $\operatorname{Im} u \oplus \operatorname{Ker} u$

Soit u un endomorphisme d'un ev E admettant un polynôme annulateur P tel que $P'(0) \neq 0$. Montrer que $\operatorname{Ker} u$ et $\operatorname{Im} u$ sont en somme directe.

Solution proposée.
Soit $P = \sum_{i=0}^{n} a_i X^i$ le polynôme considéré. On a donc
$$a_n u^n + ... + a_1 u + a_0 \operatorname{Id} = 0$$
avec $a_1 \neq 0$.

[1] *ni un multiple scalaire d'un projecteur*

Soit $y \in \operatorname{Ker} u \cap \operatorname{Im} u$. On a donc $\left\{ \begin{array}{c} \exists x \in E,\ y = u(x) \\ u(y) = 0 \end{array} \right.$, d'où

$$\left\{ \begin{array}{l} u^m(y) = 0 \ \forall m \geq 1 \\ u^m(x) = 0 \ \forall m \geq 2 \end{array} \right. .$$

En évaluant $P(u) = 0$ en y puis en x, on trouve

$$\left\{ \begin{array}{c} a_0 y = 0 \\ a_1 u(x) + a_0 x = 0 \end{array} \right. .$$

Si $a_0 \neq 0$, la première ligne fournit $y = 0$ et on a terminé, sinon la seconde ligne donne $a_1 u(x) = 0$, *i. e.* $y = u(x) = 0$ (c'est là qu'intervient l'hypothèse $a_1 \neq 0$) et là aussi c'est terminé.

Remarque. On retrouve ainsi le résultat classique sur les projecteurs avec le polynôme $X^2 - X$.

La condition trouvée est en fait nécessaire en dimension finie, comme on le montre sur la feuille sur la dimension.

On pourra également éclairer cet exercice sous la lumière de la proposition[2]

$$\textit{en dimension finie, } \operatorname{Im} u \oplus \operatorname{Ker} u = E \iff \operatorname{val} \mu_u \leq 1.$$

En effet, les hypothèses de l'énoncé se traduisent par « il y a un polynôme annulateur dont la valuation est ≤ 1 », ce qui implique que la valuation du polynôme minimal (qui divise tout polynôme annulateur) soit également ≤ 1.

3 Combinatoire dans un ev sur un corps fini

Soit $n \geq 1$ et K un corps fini de cardinal $q \geq 2$.

1. *Déterminer le nombre de droites de K^n.*
2. *Déterminer le nombre de plans de K^n.*

Solution proposée.

1. Notons $\mathcal{D}$ l'ensemble des droites de K^n. Puisqu'une droite est l'engendré Kx d'un vecteur x non nul de K^n, il est naturel de considérer l'application surjective

$$\Delta : \left\{ \begin{array}{ccc} K^n \backslash \{0\} & \twoheadrightarrow & \mathcal{D} \\ x & \longmapsto & Kx \end{array} \right.$$

et de chercher combien d'antécédents par Δ possède une droite donnée :

$$\Delta(x) = \Delta(y) \implies Kx = Ky \implies y = 1x \in Kx \implies y \in K^* x \qquad \text{car } y \neq 0\,;$$

il est en outre immédiat que deux vecteurs colinéaires non nul engendrent une même droite, de sorte qu'une droite a exactement $\#(K^*)$ antécédents par Δ. En appliquant le lemme du berger, on obtient le nombre de droites dans K^n :

$$\#\mathcal{D} = \frac{\#(K^n \backslash \{0\})}{\#(K^*)} = \frac{q^n - 1}{q - 1} = 1 + q + q^2 + ... + q^{n-1}.$$

2. On procède de même pour le nombre de plans. En notant $\mathcal{P}$ l'ensemble des plans de K^n et $\mathcal{L}$ l'ensemble des couples libres de K^n, on considère l'application surjective

$$\Pi : \left\{ \begin{array}{ccc} \mathcal{L} & \twoheadrightarrow & \mathcal{P} \\ (x, y) & \longmapsto & Kx + Ky \end{array} \right. .$$

On cherche le nombre d'antécédents d'un plan fixé :

$$\begin{aligned} \Pi(x, y) = \Pi(u, v) \quad & \implies \quad Kx + Ky = Ku + Kv \implies \left\{ \begin{array}{l} x = au + bv \\ y = cu + dv \end{array} \right. \text{ avec } a, b, c, d \in K \\ & \implies \quad ay - cx = (ad - bc)\, v \implies ad \neq bc \qquad \text{car } v \neq 0 \text{ et } (x, y) \text{ est libre}\,; \end{aligned}$$

[2] *cf.* feuilles sur la dimension finie et sur la réduction

réciproquement, si l'on peut écrire $\left\{\begin{array}{l} x = au+bv \\ y = cu+dv \end{array}\right.$ où a,b,c,d sont des scalaires tels que $ad \neq bc$, alors $\Pi(x,y)$ est clairement inclus dans $\Pi(u,v)$, et la condition $ad \neq bc$ permet d'obtenir l'inclusion inverse en écrivant $\left\{\begin{array}{l} u = \frac{d}{ad-bc}x - \frac{b}{ad-bc}y \\ v = -\frac{c}{ad-bc}x + \frac{a}{ad-bc}y \end{array}\right.$. Par ailleurs, deux tels quadruplets (a,b,c,d) distincts induisent des couples (x,y) distincts. Il en résulte que le nombre d'antécédents d'un plan donné est[3]

$$\#\left\{(a,b,c,d) \in K^4 \ ; \ ad \neq bc\right\}.$$

Pour calculer ce nombre, on commence par choisir (a,b) parmi les couples de K^2 distincts de $(0,0)$, ce qui fait q^2-1 choix. On considère ensuite à $(a,b) \neq (0,0)$ donné l'application

$$\delta : \left\{\begin{array}{ccc} K^2 & \longrightarrow & K \\ (c,d) & \longmapsto & ad-bc \end{array}\right. ;$$

on cherche le cardinal de $\delta^{-1}(K^*)$. δ est surjective car tout $x \in K$ s'écrit $\delta\left(-\frac{x}{b},0\right)$ ou $\delta\left(0,\frac{x}{a}\right)$ selon que a ou b est $\neq 0$. Pour calculer le nombre d'antécédents par δ d'un $x \in K$ fixé, on peut remarquer que l'une des applications

$$\left\{\begin{array}{ccc} K & \longrightarrow & \delta^{-1}(\{x\}) \\ c & \longmapsto & \left(c, \frac{x+bc}{a}\right) \end{array}\right. \text{ ou } \left\{\begin{array}{ccc} K & \longrightarrow & \delta^{-1}(\{x\}) \\ d & \longmapsto & \left(\frac{ad-x}{b}, d\right) \end{array}\right.$$

est bien définie et bijective, d'où $\#\left(\delta^{-1}(\{x\})\right) = q$. On en déduit que le nombre de couples (c,d) de K^2 vérifiant $ad \neq bc$ vaut q^2-q (il y a K^2 tout entier privé des antécédents de 0). Finalement, le nombre d'antécédents d'un plan donné par Π est

$$\#\left\{(a,b,c,d) \in K^4 \ ; \ ad \neq bc\right\} = \left(q^2-1\right)\left(q^2-q\right).$$

Il reste à calculer le cardinal de $\mathcal{L}$: le premier élément x d'un couple (x,y) libre peut être pris quelconque dans $K^n \backslash \{0\}$, ce qui fait q^n-1 choix, puis y peut être pris n'importe où en dehors de la droite Kx, ce qui fait q^n-q choix, d'où

$$\#\mathcal{L} = (q^n-1)(q^n-q).$$

Concluons :

$$\#\mathcal{P} = \frac{\#\mathcal{L}}{\#\left\{(a,b,c,d) \in K^4 \ ; \ ad \neq bc\right\}} = \frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)} = \frac{1+q+...+q^{n-1}}{1+q}\left(1+q+...+q^{n-2}\right).$$

Remarque. Cet exercice peut se rédiger de manière beaucoup moins hideuse à l'aide de connaissances élémentaires sur la théorie de la dimension[4].

4 Calcul d'ev engendrés par des fonctions

On se place dans l'ev des applications de $[0,1]$ dans $\mathbb{R}$.
Pour un réel a, on pose[5]

$$\begin{array}{rcl} p_a := |\cdot - a| & : & x \mapsto |x-a|, \\ s_a := \chi_{]a,1]} & : & x \mapsto \left\{\begin{array}{l} 0 \ si \ x \leq a \\ 1 \ si \ x > a \end{array}\right. , \\ s^a := \chi_{[a,1]} & : & x \mapsto \left\{\begin{array}{l} 0 \ si \ x < a \\ 1 \ si \ x \geq a \end{array}\right. . \end{array}$$

1. *Décrire le $\mathbb{R}$-ev engendré par les p_a pour $a \in [0,1]$.*

[3] Le lecteur familier des matrices remarquera que l'on a, sans le dire, inversé la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

[4] *cf.* feuille sur la dimension finie

[5] p comme « **p**ic » et s comme « **s**aut »

2. *Décrire le $\mathbb{R}$-ev engendré par les s_a et les s^a pour $a \in [0,1]$.*

Solution proposée.

1. Il est immédiat que toute combinaison linéaire des p_a est une fonction affine par morceaux continue. On va montrer l'inclusion réciproque, à savoir que $\mathrm{Vect}_{a\in[0,1]}\{p_a\}$ est exactement l'espace des fonctions affines par morceaux continues sur $[0,1]$, chaque p_a dans $f = \sum \lambda_a p_a$ correspondant à un pic du graphe de f.

   Soit donc f affine par morceaux continue. On voit que f est entièrement caractérisée par ses pics $0 = a_0 < a_1 < ... < a_{n-1} < a_n = 1$ ($n \geq 1$), ses pentes γ_i sur $]a_{i-1}, a_i[$ pour $i = 1, ..., n$ et sa valeur $f(0)$: pour le voir, parcourir le graphe de f en partant de 0. On cherche alors à écrire f sous la forme $\sum_{i=0}^n \lambda_i p_{a_i}$. En dérivant sur chaque $]a_{i-1}, a_i[$ et en considérant la condition en 0, on doit avoir le système

$$(S) : \begin{cases} \gamma_1 = \lambda_0 - \lambda_1 - \lambda_2 - ... - \lambda_n \\ \gamma_2 = \lambda_0 + \lambda_1 - \lambda_2 - ... - \lambda_n \\ \vdots \\ \gamma_n = \lambda_0 + \lambda_1 + \lambda_2 + ... + \lambda_{n-1} - \lambda_n \\ f(0) = \lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n \end{cases}.$$

   Il se trouve que (S) est également une condition suffisante pour retrouver f : il est clair que pour de tels λ_i la dérivée de $f - \sum_{j=0}^n \lambda_j p_{a_j}$ vaut 0 sur chaque $]a_{i-1}, a_i[$, donc f coïncide avec $\sum_{j=0}^n \lambda_j p_{a_j}$ sur chaque $]a_{i-1}, a_i[$ modulo une constante c_i, qui sont toutes les mêmes par continuité, et la condition initiale $f(0) = \lambda_1 |a_1| + \lambda_2 |a_2| + ... + \lambda_n |a_n|$ montre que la constante sus-citée est nulle.

   Montrons maintenant que (S) admet une solution. En soustrayant les lignes i et $i+1$ et en conservant les première et dernière lignes, on voit que (S) est équivalent à

$$\begin{cases} \gamma_2 - \gamma_1 = 2\lambda_1 \\ \gamma_3 - \gamma_2 = 2\lambda_2 \\ \vdots \\ \gamma_n - \gamma_{n-1} = 2\lambda_{n-1} \\ f(0) = \lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n \\ \gamma_1 = \lambda_0 - \lambda_1 - \lambda_2 - ... - \lambda_n \end{cases},$$

   qui donne immédiatement $\lambda_1, ..., \lambda_{n-1}$ en lisant les $n-1$ premières lignes, d'où λ_n sur l'avant-dernière ligne ($a_n = 1 \neq 0$) et λ_0 grâce à la dernière.

2. Toute combinaison linéaire des s_a et s^a est clairement une fonction en escalier. Montrons réciproquement que $\mathrm{Vect}_{a\in[0,1]}\{s_a, s^a\}$ est exactement l'espace des fonctions en escalier sur $[0,1]$, chaque s_a ou s^a dans $f = \sum \lambda_a p_a$ correspondant à un saut du graphe de f.

   Soit f en escalier sur $[0,1]$ et $0 = a_0 < a_1 < ... < a_{n-1} < a_n = 1$ ($n \geq 1$) une subdivision adaptée à f – noter que f peut prendre n'importe quelle valeur en les a_i. Il est alors judicieux de remarquer que les s_a sont à peu de choses près les dérivées des p_a ; en posant $F(x) = \int_0^x f$, on voit que F est affine par morceaux (et continue) avec la subdivision associée $a_0 < ... < a_n$, donc s'écrit $F = \sum_{i=0}^n \lambda_{a_i} p_{a_i}$ par ce qui précède. Sur le gruyère $[0,1] \backslash \{a_0, ..., a_n\}$, les p_{a_i} sont dérivables de dérivée $p'_{a_i} = 2s_{a_i} - 1$, d'où (en remarquant que $s^0 = 1$)

$$f(x) = F'(x) = \sum_{i=0}^n \lambda_{a_i} \left(2s_{a_i} - s^0\right)$$

   pour $x \in [0,1] \backslash \{a_0, ..., a_n\}$.

   Il reste les points de discontinuité : il suffit pour régler leur compte de remarquer que $s^a - s_a$ vaut 1 en a et 0 ailleurs (c'est le *Dirac* en a), donc on rajoute à l'expression précédente des multiples adéquats de $s^{a_i} - s_{a_i}$ pour corriger la valeur de f en a_i, opération qui ne modifie d'ailleurs la valeur de f *que* en a_i. Après cela, il apparaît clairement que f est engendrée par les s_a et s^a.

5 Centre de $L(E)$

Soit E un ev. On rappelle au besoin qu'un sev admet toujours un supplémentaire[6].

1. *Déterminer le centre[7] de $L(E)$.*

[6] *cf.* les derniers exercices de cette feuille pour une démonstration

[7] Le *centre* d'un anneau A est l'ensemble des $a \in A$ qui commutent avec tous les éléments de A.

2. *Trouver les endomorphismes dont le commutant*[8] *est réduit aux homothéties.*

Solution proposée.

1. Soit f dans le centre de $L(E)$. Pour un $x \in E$ donnée, on considère la projection π sur Kx parallèlement à un supplémentaire. On a alors
$$f(x) = f(\pi(x)) = \pi(f(x)) \in Kx,$$
donc $f(x) = \lambda_x x$ pour un certain $\lambda_x \in K$, et il est alors classique que f est une homothétie. Réciproquement, il est trivial que les homothéties sont dans le centre de $L(E)$.
2. Soit u un tel endomorphisme. Puisque u commute avec u, l'endomorphisme u est une homothétie, donc commute avec tout le monde, en particulier avec n'importe quel endomorphisme qui n'est pas une homothétie (on peut en trouver dès que l'ev E est de dimension > 1), ce qui est une contradiction. L'ensemble cherché est donc : ou bien le vide $\emptyset$, ou bien $L(E)$ pour $\dim E \leq 1$.

6 Liberté de formes linéaires et intersections d'hyperplans

1. *Montrer que deux formes linéaires de même noyau sont colinéaires.*
2. *Montrer qu'une forme linéaire est engendrée par une famille libre finie de formes linéaires ssi elle s'annule sur l'intersection de leur noyaux.*

Solution proposée.
Notons E l'ev considéré.

1. Soient φ et ψ dans E^* telles que $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$. Pour utiliser cette dernière hypothèse, on va construire des vecteurs qui tomberont à coup sûr dans $\operatorname{Ker}\varphi$. Comment faire ?

   L'intérêt des formes linéaires est que leurs images sont des scalaires, ce qui permet de normaliser des vecteurs : le vecteur $\frac{a}{\varphi(a)}$ est ainsi toujours envoyé sur 1 pourvu que son image $\varphi(a)$ soit non nulle. En observant subtilement que $0 = 1 - 1$, on construit ainsi plein d'éléments $\frac{a}{\varphi(a)} - \frac{b}{\varphi(b)}$ dans $\operatorname{Ker}\varphi$. Pour ne pas s'embêter avec les conditions sur les noyaux, il suffit de considérer $\varphi(b)\, a - \varphi(a)\, b$.

   Ce dernier élément tombe dans $\operatorname{Ker}\psi$, ce qui s'écrit (en fixant a et en faisant varier b)
$$\psi(a)\,\varphi - \varphi(a)\,\psi = 0.$$
   Pour conclure à la colinéarité de φ et ψ, il reste à choisir un élément a tel que $\varphi(a)$ ou $\psi(a)$ soit non nul. Si celà n'était pas possible, φ et ψ seraient nulles, *a fortiori* colinéaires, *CQFD.*
2. Traduisons l'énoncé : on prend $k \geq 1$ un entier, $\varphi_1, ..., \varphi_k$ des formes linéaires libres dans E^* et ψ une forme linéaire (quelconque) sur E ; on veut montrer l'équivalence
$$\psi \in \operatorname{Vect}\{\varphi_1, ..., \varphi_k\} \iff \bigcap_{i=1}^{k} \operatorname{Ker}\varphi_i \subset \operatorname{Ker}\psi.$$
   Le sens $\boxed{\implies}$ est trivial. On montre l'autre sens $\boxed{\impliedby}$ par récurrence sur k.

   Pour $k = 1$, on reprend la démonstration du premier point : supposant $\operatorname{Ker}\varphi \subset \operatorname{Ker}\psi$, la forme φ est libre, donc non nulle, donc on peut trouver un $a \in E \backslash \operatorname{Ker}\varphi$; le vecteur $x - \frac{\varphi(x)}{\varphi(a)} a$ est alors dans $\operatorname{Ker}\varphi$ donc dans $\operatorname{Ker}\psi$, ce qui s'écrit $\psi(x) = \frac{\varphi(x)}{\varphi(a)} \psi(a)$, d'où (en faisant varier x) $\psi = \frac{\psi(a)}{\varphi(a)} \varphi$, *CQFD.*

   Supposons le résultat vrai pour $k - 1 \geq 1$, et soient $\varphi_1, ..., \varphi_k, \psi$ des formes linéaires vérifiant les hypothèses. Nous proposons deux méthodes pour conclure.

   (a) La première consiste à raisonner comme dans cas $k = 1$, en considérant un élement
$$x - \sum_{i=1}^{k} \frac{\varphi_i(x)}{\varphi_i(x_i)} x_i,$$

[8] Le *commutant* d'une partie P d'un anneau A est l'ensemble des $a \in A$ qui commutent avec tous les éléments de P. Par exemple, le commutant de A est son centre.

que l'on aimerait être dans $\bigcap_{i=1}^{k} \operatorname{Ker} \varphi_i$ car alors il serait dans $\operatorname{Ker} \psi$ et on aurait

$$\psi = \sum_{i=1}^{k} \frac{\psi(x_i)}{\varphi_i(x_i)} \varphi_i, \ \textit{CQFD.}$$

Pour pouvoir considérer un tel élément, il faut déjà que $x_i \notin \operatorname{Ker} \varphi_i$ pour pouvoir diviser par $\varphi_i(x_i)$. Voyons ensuite comment faire en sorte qu'il soit dans tous les noyaux. À i fixé, on voudrait pouvoir ramener l'élément

$$x - \sum_{j=1}^{k} \frac{\varphi_j(x)}{\varphi_j(x_j)} x_j$$

au cas déjà traité, mettons en

$$x - \frac{\varphi_i(x)}{\varphi_i(x_i)} x_i,$$

qui est dans $\operatorname{Ker} \varphi_i$ d'après le cas $k = 1$; une manière de tuer les termes en $j \neq i$ est de prendre

$$x_i \in \operatorname{Ker} \varphi_j \text{ pour tout } j \neq i,$$

de sorte que

$$\varphi_i \left(x - \sum_{j=1}^{k} \frac{\varphi_j(x)}{\varphi_j(x_j)} x_j \right) = \varphi_i \left(x - \frac{\varphi_i(x)}{\varphi_i(x_i)} x_i \right) + \sum_{j \neq i} 0 = 0, \text{ comme souhaité.}$$

Ces deux conditions réunies (et qui suffisent à notre bonheur) équivalent à

$$x_i \in \left(\bigcap_{j \neq i} \operatorname{Ker} \varphi_j \right) \backslash \operatorname{Ker} \varphi_i \ \text{ pour tout } i.$$

Or, on peut effectivement exhiber de tels x_i pour tout i, sinon il exisiterait un i_0 tel que

$$\bigcap_{j \neq i_0} \operatorname{Ker} \varphi_j \subset \operatorname{Ker} \varphi_{i_0},$$

d'où par hypothèse de récurrence $\varphi_{i_0} \in \operatorname{Vect}_{i \neq i_0} \{\varphi_i\}$, *absurde* par liberté des φ_i.

(b) La seconde idée consiste à décrémenter le nombre de formes linéaires dans l'inclusion $\bigcap_1^k \operatorname{Ker} \varphi_i \subset \operatorname{Ker} \psi$ afin de pouvoir directement appliquer l'hypothèse de récurrence. Pour faire disparaître un sev dans l'intersection ci-dessus, il suffit d'évoquer l'identité

$$V \cap \operatorname{Ker} u = \operatorname{Ker} u_{|V}$$

valable pour u linéaire et V sev de l'ev de départ.

Prenant $V := \operatorname{Ker} \varphi_k$, on intersecte l'inclusion ci-desssus avec V, ce qui donne

$$\bigcap_1^{k-1} (V \cap \operatorname{Ker} \varphi_i) \subset V \cap \operatorname{Ker} \psi,$$

ce qui s'écrit encore (en notant des primes pour les restrictions à V)

$$\bigcap_1^{k-1} \operatorname{Ker} \varphi_i' \subset \operatorname{Ker} \psi'.$$

Par récurrence, on dispose d'une liaison $\psi' = \sum_1^{k-1} \lambda_i \varphi_i'$; la forme linéaire $\psi - \sum_1^{k-1} \lambda_i \varphi_i$ est donc nulle sur $V = \operatorname{Ker} \varphi_k$, donc colinéaire à φ_k (d'après le cas $k = 1$), *CQFD.*

Remarque. En dimension finie, un argument de dualité permet de trivialiser cette exercice . En effet, si φ est une forme linéaire, on voit rapidement que $(\operatorname{Ker}\varphi)^{\perp} = K\varphi$ dans le dual, donc on a directement

$$\bigcap_{i=1}^{k} \operatorname{Ker}\varphi_i \subset \operatorname{Ker}\psi \iff (\operatorname{Ker}\psi)^{\perp} \subset \left(\bigcap_{i=1}^{k} \operatorname{Ker}\varphi_i\right)^{\perp} \iff K\psi \subset \sum_{i=1}^{k} K\varphi_i, \text{ CQFD.}$$

En dimension infinie, l'implication $\Longleftarrow$ de gauche n'est plus valable car elle utilise implicitement la propriété $V^{\circ\perp} = V$ pour V sev du dual, propriété fausse en général[9].

Tient-elle encore si V est de dim finie ? Pour $V = \bigoplus K\varphi_i$ un tel sev, son orthogonal s'écrit $\bigcap (K\varphi_i)^{\circ} = \bigcap \operatorname{Ker}\varphi_i$. Par ailleurs, un élément ψ du dual est dans $V^{\circ\perp}$ ssi ψ s'annule sur V°, *i. e.* ssi $\bigcap \operatorname{Ker}\varphi_i \subset \operatorname{Ker}\psi$. L'énoncé dit exactement que cette dernière inclusion équivaut à $\psi \in \operatorname{Vect}\{\varphi_i\} = V$, autrement dit que l'égalité $V^{\circ\perp} = V$ reste valable pour V de dim finie.

7 Sur les réunions finies de sev stricts et le théorème de l'élément primitif

1. *Soit E un ev sur un corps K infini. Montrer que des sev stricts en nombre fini ne peuvent recouvrir l'espace E tout entier.*
2. *Soit K un corps infini et L une extension finie*[10] *de K. On suppose de plus qu'il n'y a qu'un nombre fini d'extensions intermédiaires entre K et L. Montrer qu'il y a un $a \in L$ tel que*[11] *$L = K(a)$.*

Solution proposée.

1. Supposons par l'absurde qu'il y ait $n \geq 1$ sev stricts $F_1, ..., F_n$ tels que $F_1 \cup ... \cup F_n = E$. On choisit une telle famille minimisant n. Bien que cela ne soit pas nécessaire pour la suite, on observera que l'on peut supposer sans nuire à la généralité que tous les F_i sont des hyperplans (en effet, tout sev strict est inclus dans un hyperplan).

   $F_1, ..., F_{n-1}$ ne recouvrant pas E, on peut trouver un vecteur u dans E hors de $F_1 \cup ... \cup F_{n-1}$, qui est donc dans F_n ; F_n étant par ailleurs un sev strict, il existe un point a hors de F_n.

   Un dessin dans le cas où $E = \mathbb{R}^3$ et où les F_i sont tous des plans nous permet d'intuiter que la droite affine $\Delta = a + Ku$ ne va couper les F_i qu'une fois chacun, ce qui posera un problème de cardinaux, une droite étant toujours en bijection avec le corps de base. Montrons cela proprement.

   Soit $a + \lambda u$ et $a + \mu u$ deux points de Δ supposés sur un même F_i. Leur différence $(\lambda - \mu) u$ reste donc dans F_i, ce qui impose $\lambda = \mu$ pour $i < n$ puisque $u \notin F_1 \cup \cdots \cup F_{n-1}$, d'où l'égalité des points considérés ; quant à l'intersection avec F_n, puisque $u \in F_n$, la présence d'un point $a + \lambda u$ de Δ dans F_n imposerait à $a = (a + \lambda u) - \lambda u$ d'être dans F_n, ce qui impossible par définition de a.

   On a finalement montré
$$\forall i = 1, ..., n,\ \#(F_i \cap \Delta) \leq 1,$$
   d'où
$$\begin{aligned} \#\Delta &= \#(\Delta \cap E) = \#(\Delta \cap (F_1 \cup ... \cup F_n)) = \#((\Delta \cap F_1) \cup ... \cup (\Delta \cap F_n)) \\ &\leq \#(\Delta \cap F_1) + ... + \#(\Delta \cap F_n) \leq 1 + ... + 1 = n, \end{aligned}$$
   absurde car le corps de base a été pris infini.
2. Recouvrons l'extension L par plein d'extensions intermédiaires
$$L = \bigcup_{x \in L} K(x).$$

[9] Pour un contre-exemple, prendre $E = K[X]$ et V l'engendré les $P \mapsto P^{(n)}(0)$. L'orthogonal de V est réduit à $\{0\}$ par la formule de Taylor, donc $V^{\circ\perp} = E^*$, mais pourtant la forme linéaire « évaluation en 1 » qui est aussi « somme des coefficients » n'est pas dans V (pour le voir, évaluer une éventuelle condition de liaison en deux polynômes constants).

[10] i. e. *un sur-corps de K de dimension finie sur K*

[11] *Un tel a est appelé* élément primitif *(car il engendre tout le monde).*

Puisque ces dernières sont par hypothèse en nombre fini, on peut en extraire un sous-recouvrement fini :

$$L = \bigcup_{i=1}^{n} K(x_i).$$

Les $K(x_i)$ étant des sous-K-ev de L et K étant infini, on peut appliquer ce qui précède : l'un des $K(x_i)$ doit valoir l'espace L tout entier.

Remarque. Si K est supposé fini, L est un corps fini et l'on sait alors que son groupe multiplicatif est cyclique, disons $L^* = \langle a \rangle$. On en déduit $L = K(a)$ et le théorème reste valable.

L'hypothèse sur la finitude du nombre d'extensions intermédiaires est en fait très artificielle. Le cadre naturelle est celui des extensions *séparables*. Un polynôme est dit *séparable* si ses racines dans toute extension sont simples, *i. e.* s'il est premier avec sa dérivée. Une extension finie est dite *séparable* si tous ses éléments ont un polynôme minimal séparable. On peut montrer qu'on est séparable dès qu'on est de caractéristique nulle, ce qui est le cas des extensions usuelles sur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$...

Pour montrer l'idée de pourquoi les extensions finies séparables n'ont qu'un nombre fini de sous-corps, nous allons faire une petite excursion au pays de Galois[12]. Déjà, il faut savoir qu'on peut toujours plonger une extension finie séparable dans une extension galoisienne. Sans savoir ce qu'est une extension galoisienne, il faut par ailleurs savoir que Galois a mis en bijection les sous-corps d'une extension galoisienne avec les sous-groupes du groupe de Galois de cette extension, lequel est *fini*. Cela montre que les extensions intermédiaires d'une extension galoisienne sont en nombre fini, *a fortiori* celles d'une extension finie séparable.

Le résultat de l'exercice s'énonce alors : *toute extension finie séparable est monogène.*

8 Tout ev admet une base ; tout sev admet un supplémentaire

Soit E un ev.

On dit qu'une famille finie $(x_1, ..., x_n)$ d'éléments de E est *libre* si pour tout n-uplet de scalaires $(\lambda_1, ..., \lambda_n)$ on a l'implication

$$\lambda_1 x_1 + ... + \lambda_n x_n = 0 \implies \lambda_1 = ... = \lambda_n = 0$$

(ce qui revient à dire qu'aucun des x_i n'est engendré par les autres).

Une famille $(x_i)_{i \in I}$ d'éléments de E est dite *libre* si toute sous-famille finie est libre, *génératrice* si tout $x \in E$ est engendré par un nombre fini de x_i. Une *base* de E est une famille génératrice et libre.

Soit X un ensemble ordonné. On appelle *chaîne* de X toute partie de X totalement ordonée pour l'ordre induit. Le lemme de Zorn affirme que si toute chaîne admet un majorant dans X, alors X admet un élément maximal.

Cet énoncé est extrèmement puissant[13]. En substance, il dit que, pour chercher un élément maximal dans un ensemble ordonné X, on peut s'autoriser d'une part à prendre X *totalement ordonné* (c'est le rôle des chaînes), ce qui permet au passage de confondre élément maximal et maximum, *i. e.* majorant de X dans X, d'autre part à chercher ce majorant *non nécessairement dans* X (le majorant de la chaîne ne doit pas forcément rester dans la chaîne), ce qui donne une grande liberté de manœuvre.

1. *Montrer qu'une base de E est une famille libre de E maximale pour l'inclusion.*
2. *En déduire, à l'aide du lemme de Zorn, que E admet un base.*
3. *Montrer à l'aide du lemme de Zorn que tout sev de E admet un supplémentaire dans E.*

Solution proposée.

1. Soit L libre et génératrice. Soit L' une famille libre contenant L. Si il y a un $x \in L'$ qui n'est pas dans L, puisque L est génératrice, x est engendré par un nombre fini de $x_i \in L$, mettons $x = \sum_{i=1}^{n} \lambda_i x_i$, ce qui est absurde par liberté de la sous-famille finie $(x_1, ..., x_n, x)$ de L'.

   Réciproquement, soit L une famille libre maximale. Si L n'est pas génératrice, il y a un $x \in E$ qui n'est pas engendré par L. On vérifie alors que $L \cup \{x\}$ est libre, ce qui mènera à une contradiction puisque

[12] Pour plus de détail, le lecteur est invité à consulter les notes de cours de Marc Rosso.

[13] Pour une démonstration, *cf.* feuille sur ensembles & applications.

$L \subsetneq L \cup \{x\}$ est supposée maximale pour l'inclusion : si $(x_0, x_1, ..., x_n)$ est une famille finie de $L \cup \{x\}$, ou bien elle ne contient pas x, donc est une sous-famille finie de L, donc est libre, ou bien elle contient x, mettons $x = x_0$, et alors pour des scalaires $\lambda_0, ...\lambda_n$ on a

$$\begin{aligned}\lambda_0 x + \sum_{i=1}^{n} \lambda_i x_i = 0 \quad &\Longrightarrow \quad \lambda_0 = 0 \text{ sinon } x \in \operatorname{Vect}\{x_1, ..., x_n\} \\ &\Longrightarrow \quad \sum_{i=1}^{n} \lambda_i x_i = 0 \\ &\Longrightarrow \quad \lambda_1 = ... = \lambda_n = 0 \text{ par liberté de } (x_1, ..., x_n).\end{aligned}$$

2. Une base étant une famille libre maximale pour l'inclusion, il est naturel d'essayer de zornifier l'ensemble $\mathcal{L}$ des familles libres L sur E ordonné par l'inclusion. Si l'on y parvient, on disposera d'une famille libre maximale, *i. e.* d'une base.

   Soit $\mathcal{C}$ une chaine de $\mathcal{L}$. On cherche un majorant de $\mathcal{C}$ pour l'inclusion. Un bon candidat est la famille $L_0 = \bigcup_{L \in \mathcal{C}} L$; montrons qu'elle est bien dans $\mathcal{L}$, *i. e.* que L_0 est libre. Soit $(x_1, ..., x_n)$ une sous-famille finie de L_0 ; chaque x_i est dans un $L_i \in \mathcal{C}$, et en posant $L' = \max\{L_1, ..., L_n\}$ (possible car $\mathcal{C}$ est totalement ordonnée), il est clair que tous les x_i sont dans L'. Puisque $L' \in \mathcal{C} \subset \mathcal{L}$, L' est libre, toute sous-famille finie – *a fortiori* $(x_1, ..., x_n)$ – est libre, *CQFD*.

3. Soit F un sev de E. Montrons qu'un supplémentaire de F peut être vu comme un sev S maximal en somme directe avec F.

   Si S est un sev maximal pour la propriété $F + S = F \oplus S$, on a nécessairement $F + S = E$, sinon il y aurait un $x \in E$ hors de $S + F$, et on vérifierait alors aisément que $S + Kx$ est en somme directe avec F, ce qui contredirait la maximalité de S.

   Si S est un supplémentaire de F, soit S' un sev contenant S tel que $F + S' = F \oplus S'$. Puisque $E = S \oplus F$, tout élémement $s' \in S'$ s'écrit $s' = s + f$ avec $s \in S \subset S'$, et la décomposition est unique dans $F \oplus S'$, ce qui montre que $f = 0$ et donc $s' = s \in S$; on en déduit $S' = S$, ce qui prouve que S est maximal pour la propriété $F + S = F \oplus S$.

   On va par conséquent zornifier l'ensemble $\mathcal{S}$ des sev S en somme directe avec F, ce qui montrera l'existence d'un supplémentaire pour F d'après ce qui précède.

   Soit $\mathcal{C}$ une chaine de $\mathcal{S}$. L'ensemble $S_0 = \bigcup_{S \in \mathcal{C}} S$ majore trivialement $\mathcal{C}$; montrons que S_0 est bien dans $\mathcal{S}$, *i. e.* que S_0 est un sev en somme directe avec F. Il est déjà clair que

$$F \cap S_0 = F \cap \bigcup_{S \in \mathcal{C}} S = \bigcup_{S \in \mathcal{C}} \underbrace{(F \cap S)}_{=\{0\} \text{ car } S \in \mathcal{C} \subset \mathcal{S}} = \{0\}.$$

   Si de plus x et y sont dans S_0, mettons $\left\{\begin{array}{l} x \in S_x \in \mathcal{C} \\ y \in S_y \in \mathcal{C} \end{array}\right.$, alors x et y sont dans le sev $S' = \max\{S_x, S_y\}$, donc toute combinaison linéaire de x et y reste dans $S' \subset S_0$, ce que montre que S_0 est un sev, *CQFD*.

Remarque. Le lemme de Zorn est en fait, modulo les autres axiomes de la théorie des ensembles (nommés ZF, pour Zermelo Fraenkel), équivalent à l'axiome du choix, dont Kurt Gödel et Paul Cohen ont montré respectivement dans les années 30 et 60 que l'ajout *ou* l'ajout de sa négation aux axiomes de ZF n'apportait pas de contradiction[14]. Accepter Zorn est par conséquent une affaire de croyance, ou plus simplement... de choix !

Malgré la puissance du lemme de Zorn, la plupart des résultats démontrés par zornification sont des résultats d'existence dont il est quasi-impossible d'exhiber des êtres concrêts. On pourra à ce sujet essayer (pas trop longtemps quand même...) d'exhiber une $\mathbb{Q}$-base de $\mathbb{R}$ (appelée base de *Hamel*) ou bien une $\mathbb{R}$-base de $\mathbb{R}^{\mathbb{N}}$ (espace des suites réelles). On se trouve également face à des résultats surprenant, comme l'existence d'ensembles non-mesurables pour la mesure de Lebesgue, qui sont à la source d'énoncés très déroutant. On évoquera le paradoxe de Banach-Tarski qui, interprété dans le langage courant, implique que l'on peut découper une boule en parties et recomposer ses parties pour former une boule aussi grosse que voulue, rendant ainsi possible (entre autres) la multiplication des pains.

[14] s'il n'en existait pas déjà auparavant

9 Théorème de Maschke

Soit E un $\mathbb{R}$-ev et G un sous-groupe fini de $GL(E)$. On suppose donné un sev F de E stable[15] *par G. Montrer qu'il existe un supplémentaire de F qui est lui aussi stable par G.*

On pourra considérer le projecteur sur F parallèlement à un supplémentaire et remarquer que, pour un endomorphisme u donné, l'endomorphisme $\frac{1}{|G|}\sum_{g\in G} gug^{-1}$ commute avec G.

Solution proposée.

Soit S un supplémentaire quelconque de F :

$$E = F \oplus S.$$

On peut toujours écrire $F = \operatorname{Ker} p$ où p est le projecteur sur F parallèlement à S. Si p commutait avec G, son noyau serait stable par G (lemme classique) et on aurait terminé. Il est par conséquent naturel de chercher à « commutativer » p en priant pour que le « commutativé » reste un projecteur d'image f (afin que son noyau reste un supplémentaire stable). L'énoncé nous y invite en considérant

$$\widehat{p} = \frac{1}{|G|}\sum_{g\in G} gpg^{-1}.$$

Vérifions que $\widehat{p}$ commute avec G : pour $g \in G$, on a bien

$$\begin{aligned} g\widehat{p}g^{-1} &= g\left(\frac{1}{|G|}\sum_{h\in G} hph^{-1}\right)g^{-1} = \frac{1}{|G|}\sum_{h\in G} ghph^{-1}g^{-1} \\ &= \frac{1}{|G|}\sum_{h\in G} (gh)\,p\,(gh)^{-1} \overset{i=gh}{=} \frac{1}{|G|}\sum_{i\in G} ipi^{-1} = \widehat{p}. \end{aligned}$$

Vérifions que $\widehat{p}$ reste un projecteur d'image F, ce qui concluera car alors

$$E = \operatorname{Im}\widehat{p} \oplus \operatorname{Ker}\widehat{p}$$

avec $\operatorname{Ker}\widehat{p}$ stable, *CQFD*. On veut $\operatorname{Im}\widehat{p} = F$, donc il faut montrer $\widehat{p}_{|F} = \operatorname{Id}_F$.

D'une part, pour $x \in F$, on vérifie que

$$\begin{aligned} \widehat{p}(x) &= \left[\frac{1}{|G|}\sum_{g\in G} gpg^{-1}\right](x) = \frac{1}{|G|}\sum_{g\in G} g\left(p\left(\underbrace{g^{-1}(x)}_{\in F \text{ car } F \text{ stable}}\right)\right) \\ &= \frac{1}{|G|}\sum_{g\in G} g\left(\underbrace{g^{-1}(x)}_{\text{car } F=\operatorname{Im} p}\right) = \frac{1}{|G|}\sum_{g\in G} x = x, \end{aligned}$$

d'où

$$\widehat{p}_{|F} = \operatorname{Id}_F \text{ et } F \subset \operatorname{Im}\widehat{p};$$

d'autre part, pour $x \in E$, on a

$$\begin{aligned} \widehat{p}(x) &= \left[\frac{1}{|G|}\sum_{g\in G} gpg^{-1}\right](x) = \frac{1}{|G|}\sum_{g\in G} g\left(\underbrace{p\left(g^{-1}(x)\right)}_{\in \operatorname{Im} p = F}\right) \\ &\in \frac{1}{|G|}\sum_{g\in G} \underbrace{g(F)}_{\subset F \text{ car } F \text{ stable}} \subset \frac{1}{|G|}\sum_{g\in G} F = F, \end{aligned}$$

d'où $\operatorname{Im}\widehat{p} \subset F$ et l'égalité

$$\operatorname{Im}\widehat{p} = F.$$

[15] i. e. *stable par tous ses éléments*

Par ailleurs, pour $x \in E$, on a

$$\widehat{p}^2(x) = \widehat{p}\left(\underbrace{\widehat{p}(x)}_{\in F}\right) = \widehat{p}(x),$$

d'où, en faisant varier x,

$$\widehat{p}^2 = \widehat{p},$$

i. e. $\widehat{p}$ projeteur. Ceci achève les vérifications.

Remarque. On peut donner une preuve entièrement différente (et beaucoup plus élégante) en mettant une structure préhilbertienne (*i. e.* un produit scalaire) sur E. Soit $\langle \cdot \mid \cdot \rangle$ un produit scalaire quelconque sur E, par exemple le produit scalaire canoniquement associé à une base. On pose alors

$$\langle x \mid y \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle g(x) \mid g(y) \rangle .$$

Il est aisé de vérifier que ce nouveau produit scalaire, d'une part est bien un produit scalaire, d'autre part est invariant par G, au sens où son groupe orthogonal contient G :

$$\forall g \in G, \forall x, y \in E, \langle g(x) \mid g(y) \rangle_G = \langle x \mid y \rangle_G .$$

Puisque F est stable par G, son orthogonal $F^\perp$ pour le produit scalaire $\langle \cdot \mid \cdot \rangle_G$ est lui-aussi stable par G :

$$\forall f^\perp \in F^\perp, \forall g \in G, \forall f \in F, \left\langle g\left(f^\perp\right) \mid f \right\rangle_G = \left\langle f^\perp \mid \underbrace{g^{-1}(f)}_{\in F} \right\rangle_G = 0.$$

Ploum.

10 Une famille libre de même cardinal que l'espace entier

On regarde $\mathbb{R}$ comme un $\mathbb{Q}$-ev. On pose $x_a := \sum_{n \geq 1} \frac{1}{10^{\lfloor a^n \rfloor}}$ pour a réel > 1.
On souhaite montrer que la famille $(x_a)_{a>1}$ est libre.

11 Un lemme

Soit $a_1, ..., a_n$ des réels > 0. On note a le plus petit des a_i.
On veut montrer que, pour tout $0 < \alpha < a$, il y a des intervalles de longueur α sans multiples de a_i arbitrairement loin de 0.

On note $/a/ := a - \lfloor a \rfloor$ la partie fractionnaire d'un réel a. On fixe un entier N.

1. *En considérant les suites de* $\left/ \frac{pN}{a_i} \right/$ *où p varie, montrer qu'il y a des entiers k, $k_1, ..., k_n$ tels que*

$$\forall i = 1, ..., n,\ |k - n_i a_i| < \frac{a_i}{N}.$$

2. *En déduire un intervalle sans multiples de a_i puis conclure.*

Solution proposée.

1. C'est une application du principe des tiroirs. On subdivise le n-cube $[0,1]^n$ en N^n petit cubes de côté $\frac{1}{N}$, dans lesquels on met l'infinité de n-uplets $\left(\left/\frac{pN}{a_1}\right/, \left/\frac{pN}{a_2}\right/, ..., \left/\frac{pN}{a_n}\right/\right)$ lorsque p décrit $\mathbb{N}$. Par le principe des tiroirs, l'un des N^n cubes va contenir deux n-uplets distincts – appelons p et q leurs indices. Les n différences $\left/\frac{pN}{a_i}\right/ - \left/\frac{qN}{a_i}\right/$ sont donc toutes majorées par $\frac{1}{N}$, ce qui s'écrit (pour un i entre 1 et n) :

$$\begin{aligned}
\left|\frac{pN}{a_i} - \left\lfloor\frac{pN}{a_i}\right\rfloor - \left(\frac{qN}{a_i} - \left\lfloor\frac{qN}{a_i}\right\rfloor\right)\right| &\leq \frac{1}{N} \\
\left|\frac{(p-q)N}{a_i} - \underbrace{\left(\left\lfloor\frac{pN}{a_i}\right\rfloor - \left\lfloor\frac{qN}{a_i}\right\rfloor\right)}_{:=k_i}\right| &\leq \frac{1}{N} \\
\left|(p-q)N - k_i a_i\right| &\leq \frac{1}{N},
\end{aligned}$$

d'où le résultat en posant $k := (p-q)N$.

2. Fixons un i entre 1 et n. Le point qui précède permet d'encadrer le multiple $k_i a_i$ selon

$$k - \frac{a_i}{N} \leq k_i a_i \leq k + \frac{a_i}{N}.$$

On en déduit immédiatement un encadrement du multiple suivant :

$$k + \left(1 - \frac{1}{N}\right) a_i \leq (k_i + 1) a_i \leq k + \left(1 + \frac{1}{N}\right) a_i.$$

Par conséquent, il n'y pas de multiples de a_i dans l'intervalle $\left]k + \frac{a_i}{N}, k + \left(1 - \frac{1}{N}\right) a_i\right[$. L'intersection de ces n invervalles, qui s'écrit $\left]k + \frac{A}{N}, k + \left(1 - \frac{1}{N}\right) a\right[$ avec $A := \max a_i$, ne contient donc aucun multiples d'aucun a_i.

Par ailleurs, sa longueur $\left(1 - \frac{1}{N}\right) a - \frac{A}{N}$ sera plus grande que α ssi $a - \frac{a+A}{N} > \alpha$, ce qui réalisé pour N assez grand vu que $\alpha < a$. Enfin, l'entier k peut être pris aussi grand que voulu puisqu'il vérifie $k = (p-q)N \geq N$ quitte à imposer rétrospectivement $p > q$.

12 La liberté des x_a

On suppose par l'absurde que les x_a sont $\mathbb{Q}$-liés.

1. *Montrer que l'on peut écrire*

$$\sum_{i=1,\ldots,p} u_i x_{a_i} = \sum_{j=1,\ldots,q} v_j x_{b_j}$$

où les a_i, b_j sont des réels > 1 et les u_i, v_j sont des entiers > 0.

On renomme les a_i et b_j puis on les ordonne comme suit :

$$1 < a < a_1 < a_2 < ... < a_r.$$

2. *Montrer qu'il y a une longueur $L > 1$ pour laquelle on peut trouver des intervalles $\left[a^x, a^{x+L}\right]$ ne contenant aucune puissance entière des a_i avec x réel arbitrairement grand.*

On pose $L' := \frac{1+L}{2}$, puis pour x réel $n_x := \lfloor x + L' \rfloor$ et $I_x := [a^x, \lfloor a^{n_x} \rfloor]$.

3. *Montrer que l'intervalle I_x peut être rendu arbitrairement large.*
4. *Montrer que l'intervalle I_x ne contient aucun entier de la forme $\lfloor a_i^n \rfloor$ où $n \in \mathbb{N}$.*

5. *Conclure.*

Solution proposée.

1. Soit une relation de $\mathbb{Q}$-liaison entre les x_α. Pour trouver la forme voulue, il suffit de tuer les dénominateurs et de séparer les coefficients positifs des négatifs.

   On remarque que les trous (suite de zéros consécutifs) dans l'écriture décimale de x_α sont de taille qui diverge de façon (presque) géométrique. Ainsi, pour obtenir les décimales lointaines d'un x_α multiplié par un entier u, il suffit de subsitiuter l'entier u aux chiffres 1 situés aux décimales du type $\lfloor \alpha^n \rfloor$. Pour éviter les chevauchement d'écriture, on ne regarde que les décimales lointaines.

   L'idée est alors de trouver un intervalle $\left[\lfloor \alpha^n \rfloor, \lfloor \alpha^{n+1} \rfloor\right]$ ne contenant aucun autre exposant du type $\lfloor \beta^m \rfloor$: en lisant alors les décimales de la relation de liaison entre $\lfloor \alpha^n \rfloor$ et $\lfloor \alpha^{n+1} \rfloor$, on obtiendra celle d'un u_i (ou v_j) d'un côté et 0 de l'autre, contradiction.

2. Regardons ce qui se passe lorsqu'une puissance a_i^n se glisse dans un intervalle $\left[a^x, a^{x+L}\right]$ avec x et L des réels > 0 : passant au logarithme de base a, il vient $x < n \lg_a a_i < x + L$. Pour obtenir une contradiction, il suffit d'appliquer le lemme aux réels $\lg_a a_i > 1$ (le L donné par le lemme étant aussi proche de $\max \lg_a a_i$ que voulu, il peut être pris > 1).
3. La différence entre les longueurs des l'intervalle $[a^x, \lfloor a^{n_x} \rfloor]$ et $[a^x, a^{n_x}]$ étant majorée par $|a^{n_x} - \lfloor a^{n_x} \rfloor| \leq 1$, il est équivalent de dire que l'une ou l'autre peut être rendue aussi grande que voulu. On regarde donc la plus simple :

$$\begin{aligned} a^{n_x} - a^x &= a^x \left(a^{\lfloor x+L' \rfloor - x} - 1\right) \\ &\geq a^x \left(a^{(x+L'-1)-x} - 1\right) \text{ car } a > 1 \\ &= a^x \left(a^{L'-1} - 1\right) \\ &= a^x \left(\text{cste} > 0\right) \text{ car } L' > 1 \\ &\longrightarrow \infty \text{ quand } x \to \infty, \textit{ CQFD.} \end{aligned}$$

4. Soit par l'absurde un encadrement $a^x < \lfloor a_i^n \rfloor < \lfloor a^{n_x} \rfloor$. On récupère à droite l'inégalité $a_i^n < a^{n_x} + 1$. Si l'on majore ce dernier par a^{x+L}, on aura trouvé une puissance de a_i dans notre tranche, ce qui est impossssible d'après un point précédent. On aimerait donc l'inégalité $a^{x+L} - a^{n_x} \overset{?}{>} 1$. Or, la quantité de gauche peut être rendue arbitrairement grande[16] :

$$a^{x+L} - a^{n_x} = a^{x+L} - a^{x+L'} + \underbrace{a^{x+L'} - a^{n_x}}_{\geq 0} \geq a^x \left(a^L - a^{L'}\right) \overset{x\to\infty}{\longrightarrow} \infty \text{ car } L > L', \textit{ CQFD.}$$

5. Les points qui précédent nous permettent de disposer des encadrements

$$a^x < (\text{trou arbitrairement large}) < \lfloor a^{n_x} \rfloor < a^{n_x} < (\text{trou arbitrairement large}) < a^{x+L}$$

   avec aucune décimale de la forme $\lfloor a_i^n \rfloor$ autre que $\lfloor a^{n_x} \rfloor$.

   On va lire dans la relation $\sum u_i x_{a_i} = \sum v_j x_{b_j}$ (avec les anciens indices) les décimales à gauche de $\lfloor a^{n_x} \rfloor$. Pour éviter les chevauchements d'écriture, on choisit x de sorte que les deux trous soient de longueur plus grande que tous les u_i et v_j.

   Le réel a apparaît d'un côté (et d'un seul), mettons $a = a_{i_0}$. Alors l'entier positif u_{i_0} est non nul, donc possède un chiffre non nul, mettons le k-ième en partant de la droite. La décimale $\lfloor a^{n_x} \rfloor - k$ est donc non nulle à gauche, mais doit être nulle à droite, d'où la contradiction recherchée.

Remarque. Nous avons ainsi contruit une famille libre de même cardinal que l'espace entier !
Évidemment, de tels phénomènes sont proscrits en dimension finie : que dire en effet d'un ev de cardinal **et** dimension n ? Il devrait vérifier $n = |K|^n$ (où K est le corps de base), d'où $n \geq 2^n$ (un corps possède toujours au moins deux éléments), ce qui est impossible.

Au passage, puisque $\mathbb{R}$ contient trivialement une famille génératrice de cardinal lui-même (prendre tous les $\mathbb{R}$), on aura trouvé deux familles de même cardinal, l'une libre, l'autre liée, d'où la dimension de $\mathbb{R}$ en tant que $\mathbb{Q}$-ev :

$$\dim_{\mathbb{Q}} \mathbb{R} = \operatorname{Card} \mathbb{R}.$$

[16] L'intérêt d'avoir introduit L' apparaît clairement dans les inégalités qui suivent.