Méthodes – Polynômes
Raisonnements sur les racines

Sauf exceptionnellement pour des raisons didactiques qui apparaîtront çà et là, j'écrirai de la même manière un polynôme P et son application polynomiale associée.

1 Principe général

Rappelons la caractérisation des racines d'un polynôme. Soit $P \in K[X]$, et soit $a \in K$. Alors :

$$P(a) = 0 \iff X - a \text{ divise } P \ (\iff \exists Q \in K[X],\ P = (X-a)Q).$$

Nous avons une caractérisation analogue des racines multiples : $(X-a)^k$ divise P si et seulement si : $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ (ici k est un entier naturel non nul).

De tous les résultats à connaître sur les polynômes, c'est probablement le plus important (avec le théorème de division euclidienne, qui permet d'ailleurs de démontrer cette caractérisation), parce qu'il permet de reconstituer pas à pas un polynôme à l'aide de sa valeur en quelques points.

En effet, mettons qu'on cherche à expliciter un certain polynôme P de degré n. En principe, la donnée de ce polynôme P équivaut à la donnée de ses $n+1$ coefficients. Mais si l'on sait que P s'annule en k réels ou complexes $a_1, \ldots, a_k$, alors d'après la caractérisation rappelée ci-dessus, on peut l'écrire : $P = (X-a_1)\cdots(X-a_k)Q$, avec $\deg(Q) = n-k$: en ce cas, il n'y a non pas besoin de connaître $n+1$ coefficients de P pour l'expliciter complètement, mais seulement de connaître les $n-k+1$ coefficients de Q : plus k est grand (c'est-à-dire : plus on connaît de racines de P), et plus le nombre de coefficients inconnus $n-k+1$ est petit. Il devient donc de plus en plus facile de reconstituer P.

Le cas le plus favorable est celui où l'on connaît exactement n racines $a_1, \ldots, a_n$ de P, et la valeur de P en un $(n+1)^{\text{e}}$ nombre a_{n+1} : en ce cas, $P = Q\prod_{i=1}^{n}(X-a_i)$, et pour des raisons de degré Q doit être une **constante**, qu'on détermine grâce à la valeur connue de P en a_{n+1}. En résumé :

> Connaître un polynôme de degré n en $n+1$ évaluations permet de l'expliciter complètement.

Il faut bien se rendre compte que c'est un phénomène tout à fait extraordinaire et spécifique aux polynômes. On ne peut pas en dire autant de n'importe quelle fonction : si je vous dis qu'une fonction f s'annule en tous les entiers naturels, par exemple, pouvez-vous en déduire une forme explicite de f ? Absolument pas : ce peut tout aussi bien être la fonction nulle que $x \mapsto \sin(\pi x)$ ou $x \mapsto (\sin(\pi x))^2$, par exemple (une infinité d'autres fonctions sont possibles). Vous n'en savez rien.

Alors que dans le cas d'un polynôme, vous pouvez le reconstituer à partir d'un nombre fini d'évaluations. Cela veut dire en particulier que même si la donnée de départ est seulement qu'il est de degré 9, et sa valeur en les entiers entre 1 et 10 (par exemple), alors vous pourrez l'expliciter pour ensuite donner sa valeur en $\frac{1}{2}$, $\sqrt{\pi}$, -5... Partout. Même en des endomorphismes ou matrices ! (voir la section 5)

Nous n'avons détaillé ci-dessus que le cas où n de ces évaluations donnent zéro, pour que l'interprétation en termes de racines soit immédiate. C'est en fait valable peu importe la valeur de ces évaluations, mais c'est alors plus compliqué que ce qu'on va illustrer dans cette section : le cas général nécessite les polynômes d'interpolation de Lagrange.

C'est un principe à avoir en tête dans la mesure où, souvent, vous ne connaîtrez des polynômes que par leurs évaluations en certains réels ou complexes, et vous devrez « remonter » au polynôme de départ (on expliquera pourquoi ce peut être nécessaire dans la section 4, là où une réflexion superficielle pourrait faire penser que les applications polynomiales suffisent). Nous illustrons l'approche dans les sections suivantes.

2 Expliciter un polynôme vérifiant des conditions prescrites

Grâce à la caractérisation et aux explications de la section précédente, nous savons reconstituer petit à petit un polynôme à partir de ses racines, pourvu qu'on en connaisse suffisamment. Cependant on ne vous définira pas toujours un polynôme P en vous présentant ses racines, mais en disant qu'il vérifie une égalité du type : $\forall x \in \cdots$, $P(x) = \bigstar$ (où le membre de droite dépend souvent de x). Pour pouvoir utiliser la caractérisation des racines, vous devrez alors réarranger cette égalité en la mettant sous la forme : $\forall x \in \cdots$, $\spadesuit(x) = 0$, où $\spadesuit$ est polynomial. Cela nécessitera de soustraire $\bigstar$ à chaque membre de l'égalité supposée, mais plus encore : si la quantité n'est pas polynomiale à cause de la présence de quotients ou de racines carrées, vous devrez les éliminer (en multipliant l'égalité par les dénominateurs en présence, par exemple) : un polynôme ne fait en effet intervenir que des sommes, différents, produits et puissances entières d'une variable. Tout le reste est à exclure.

Exemple 1. Soit $n \in \mathbb{N}$, et soit P un polynôme de degré n. On suppose :

$$\forall k \in [\![0, n]\!], \quad P(k) = \frac{k}{k+1}.$$

On aimerait connaître la valeur de P en $n+1$. Pour cela, nous avons besoin de l'expliciter à partir de ses valeurs en $0, \ldots, n$: d'après les commentaires ci-dessus, ce devrait être possible (on a un polynôme de degré n, et $n+1$ évaluations). Commençons par réécrire l'égalité précédente sous la forme $\spadesuit(k) = 0$ où $\spadesuit$ est polynomial : cela nécessite d'éliminer le quotient dans le membre de droite. On y parvient après multiplication par $k+1$, et on se ramène alors à l'égalité équivalente : $\forall k \in [\![0, n]\!]$, $(k+1)P(k) - k = 0$. Cela signifie que le polynôme $(X+1)P - X$ (on a remplacé les k par des X pour reconnaître le polynôme dont on a considéré l'évaluation) admet tous les entiers $k \in [\![0, n]\!]$ pour racines. D'après la caractérisation des racines, il existe donc $Q \in \mathbb{R}[X]$ tel que :

$$(X+1)P - X = Q \prod_{k=0}^{n} (X - k),$$

et pour des raisons de degré on doit avoir : $\deg(Q) = 0$, c'est-à-dire : Q est une constante.

Pour la déterminer, on a besoin d'évaluer l'égalité précédente en un nombre où le membre de gauche est connu. Réévaluer en $k \in [\![0, n]\!]$ ne va rien nous apporter, on aura $0 = 0$, et ce n'est pas une surprise : on a déjà exploité cette information. On semble coincé parce qu'on ne connaît pas encore P en d'autres valeurs que ces entiers-là. L'idée est alors d'évaluer l'égalité $(X+1)P - X = Q \prod_{k=0}^{n} (X - k)$ en un réel qui « élimine » le terme inconnu $(X+1)P$: ceci incite à évaluer en -1. Ce faisant, on obtient : $1 = Q \prod_{k=0}^{n} (-1 - k)$, donc : $Q = \frac{1}{\prod_{k=0}^{n} (-1-k)}$. Nous vous laissons vous convaincre que le dénominateur est égal à $(-1)^{n+1}(n+1)!$, de sorte que finalement :

$$(X+1)P - X = \frac{(-1)^{n+1}}{(n+1)!} \prod_{k=0}^{n} (X - k).$$

On peut isoler P et avoir son expression explicite. Comme promis, sa valeur en $n+1$ réels a suffi à le reconstituer. Cette expression permet d'obtenir sa valeur n'importe où, bien qu'on ne la connût qu'en les entiers $k \in [\![0, n]\!]$ *a priori*. Par exemple, en évaluant en $n+1$:

$$(n+2)P(n+1) - (n+1) = \frac{(-1)^{n+1}}{(n+1)!} \prod_{k=0}^{n} (n+1-k).$$

Exercice 1. Simplifier l'expression ci-dessus pour en déduire : $P(n+1) = \dfrac{(n+1) + (-1)^{n+1}}{n+2}$.

Exemple 2. Soit $n \in \mathbb{N}$. On cherche à déterminer les polynômes $P \in \mathbb{R}[X]$ interpolant la fonction carrée en les entiers entre 0 et n, c'est-à-dire vérifiant : $\forall k \in [\![0, n]\!]$, $P(k) = k^2$. Conformément au conseil

ci-dessus, si je veux interpréter ces égalités en termes de racines, je dois soustraire k^2 de chaque côté, et me ramener à l'égalité équivalente : $\forall k \in [\![0,n]\!]$, $P(k)-k^2=0$. On en déduit que si P convient, alors le polynôme $P-X^2$ admet pour racines les entiers $k \in [\![0,n]\!]$, donc il est divisible par $X-k$ pour tout $k \in [\![0,n]\!]$. On en déduit que P convient si et seulement s'il existe $Q \in \mathbb{R}[X]$ tel que :

$$P - X^2 = \prod_{k=0}^{n} (X-k)Q,$$

si et seulement s'il existe $Q \in \mathbb{R}[X]$ tel que : $P = X^2 + \prod_{k=0}^{n}(X-k)Q$. On peut expliciter Q si l'on a davantage d'hypothèses sur P (par exemple, si $\deg(P) = n+1$ avec $n \geqslant 1$, alors Q doit être une constante, qu'on détermine grâce à la valeur de P en n'importe quel autre nombre que les entiers de $[\![0,n]\!]$).

Attention, cette méthode n'est plus aussi efficace si les évaluations que vous voulez interpréter comme l'annulation d'un polynôme, ne font pas intervenir le même polynôme à chaque fois. Par exemple, si vous voulez expliciter un polynôme P tel que $P(0)=1$, $P(1)=2$ et $P(2)=4$, alors la première égalité vous dit que $P-1$ admet 0 pour racine, tandis que la seconde égalité dit que $P-2$ admet 1 pour racine, et enfin la dernière dit que $P-4$ admet 2 pour racine : ces trois égalités permettent donc de factoriser $P-1$, $P-2$ et $P-4$, respectivement par X, $X-1$ et $X-2$, mais vous ne pouvez pas en déduire une factorisation de P (essayez pour voir où cela coince). C'est pourquoi, pour fabriquer un tel polynôme, nous avons besoin des polynômes interpolateurs de Lagrange.

2.1 Application : *fabriquer* un polynôme vérifiant « ce qu'on veut »

Lorsqu'une relation est valable pour TOUT polynôme (ou, éventuellement, tout polynôme de degré donné, unitaire, etc.), il est avantageux de regarder ce que donne cette relation, en particulier, pour des polynômes bien choisis. Par « bien choisi », il faut souvent comprendre : qui s'annule en suffisamment de réels ou complexes, pour que la relation devienne une égalité simple (avec un seul terme, idéalement, si elle faisait intervenir une somme initialement), dont on saura tirer toutes sortes d'informations. Le propos sera plus clair avec l'exemple et les exercices de cette partie.

La difficulté est alors : comment *trouver* un polynôme s'annulant en les réels qu'on veut ? Les sections précédentes nous disent comment : en interprétant une annulation en a comme une divisibilité par $X-a$, et plus généralement une annulation en $a_1, \dots, a_k$ comme une divisibilité par $\prod_{i=1}^{k}(X-a_i)$. Il suffit alors de prendre pour P un multiple de ce produit, afin qu'il vérifie les annulations requises (si ce ne sont pas des annulations que nous cherchons, alors il faut réfléchir davantage).

À partir du moment où l'on introduit les polynômes interpolateurs de Lagrange, vous savez comment trouver des polynômes s'annulant en des valeurs prescrites $a_1, \dots, a_k$. Si $(L_1, \dots, L_k)$ est la famille de polynômes interpolateurs associée à $(a_1, \dots, a_k)$, alors le polynôme :

$$L_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{X-a_j}{a_i-a_j}$$

s'annule en tous les a_j pour $j \neq i$ (et vaut 1 en a_i). Mais il peut être dispensable d'introduire ces polynômes si l'on a seulement des conditions d'annulation.

Exemple 3. Soit $d \in \mathbb{N} \setminus \{0\}$. Pour illustrer le paragraphe précédent, nous allons montrer que la famille $\left(f_0 : x \mapsto 1, f_1 : x \mapsto e^x, f_2 : x \mapsto e^{2x}, \dots, f_d : x \mapsto e^{dx}\right)$ est libre en construisant un polynôme prenant des valeurs prescrites. N'y pensons pas pour le moment, nous verrons où cela intervient. Soit $(\alpha_0, \dots, \alpha_{d+1}) \in \mathbb{R}^{d+1}$ tel que : $\sum_{i=0}^{d} \alpha_i f_i = 0$. Alors :

$$\forall x \in \mathbb{R}, \quad \alpha_0 + \alpha_1 e^x + \alpha_2 e^{2x} + \cdots + \alpha_d e^{dx} = 0.$$

Nous avons $d+1$ inconnues : conformément aux conseils de la section *Indépendance linéaire* du chapitre *Algèbre linéaire*, nous ne parviendrons pas à démontrer l'indépendance linéaire si nous ne produisons pas $d+1$ équations. Faisons-le en dérivant d fois l'équation ci-dessus. Nous obtenons alors :

$$\forall x \in \mathbb{R}, \quad \left\{ \begin{array}{ccccccccccc} \alpha_0 & + & \alpha_1 e^x & + & \alpha_2 e^{2x} & + & \cdots & + & \alpha_d e^{dx} & = & 0 \quad (L_0) \\ & & \alpha_1 e^x & + & 2\alpha_2 e^{2x} & + & \cdots & + & d\alpha_d e^{dx} & = & 0 \quad (L_1) \\ & & \alpha_1 e^x & + & 2^2\alpha_2 e^{2x} & + & \cdots & + & d^2\alpha_d e^{dx} & = & 0 \quad (L_2) \\ & & \vdots & & \vdots & & & & \vdots & \vdots & \vdots \\ & & \alpha_1 e^x & + & 2^{d-1}\alpha_2 e^{2x} & + & \cdots & + & d^{d-1}\alpha_d e^{dx} & = & 0 \quad (L_{d-1}) \\ & & \alpha_1 e^x & + & 2^d\alpha_2 e^{2x} & + & \cdots & + & d^d\alpha_d e^{dx} & = & 0 \quad (L_d) \end{array} \right.$$

Nous avons $d+1$ équations pour $d+1$ inconnues : nous pouvons en principe résoudre ce système, *via* des opérations convenables sur les lignes. Il semble délicat, à première vue, de voir quelles sont les opérations « convenables » à effectuer (rappelons que dans la section *Indépendance linéaire* du document de méthodologie d'algèbre linéaire, je vous encourage à faire des opérations, ou des évaluations, de sorte à éliminer toutes les inconnues sauf une, pour simplifier la résolution). À défaut d'avoir une idée, écrivons d'abord une combinaison linéaire arbitraire de ces lignes, avec des coefficients inconnus $a_0, \ldots, a_d$, et nous verrons plus tard comment les choisir de la façon la plus intelligente possible : si l'on fait $L_d \leftarrow a_0 L_0 + a_1 L_1 + a_2 L_2 + \cdots + a_d L_d$, on obtient :

$$\forall x \in \mathbb{R}, \quad a_0\alpha_0 + \sum_{i=0}^{d} a_i \alpha_1 e^x + \sum_{i=0}^{d} a_i 2^i \alpha_i e^{2x} + \cdots + \sum_{i=0}^{d} a_i d^i \alpha_d e^{dx} = 0.$$

On voit donc que si l'on pose : $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{R}_d[X]$, l'égalité ci-dessus équivaut à :

$$\forall x \in \mathbb{R}, \quad P(0)\alpha_0 + P(1)\alpha_1 e^x + P(2)\alpha_2 e^{2x} + \cdots + P(d)\alpha_d e^{dx} = 0. \qquad (*)$$

Comme les $a_0, \ldots, a_d$ ont été choisis arbitrairement, cette égalité vaut pour TOUT polynôme $P \in \mathbb{R}_d[X]$. En particulier, si l'on parvient à trouver un polynôme P qui annule tous les termes de $(*)$ sauf un, alors ce choix de polynôme nous ramène à une équation extrêmement simple avec une seule inconnue. Pour cela, soit $(L_0, L_1, \ldots, L_d)$ la famille des polynômes interpolateurs de Lagrange associée à $(0,1,\ldots,d)$. Soit $i \in [\![1, d]\!]$. On rappelle que l'on a par définition : $\forall j \in [\![0, d]\!] \setminus \{i\}$, $L_i(j) = 0$, et : $L_i(i) = 1$. Par conséquent, si l'on prend $P = L_i$ dans $(*)$, alors cette égalité devient : $\forall x \in \mathbb{R}$, $L_i(i)\alpha_i e^{ix} = 0$ (tous les autres termes s'annulent du fait que $L_j(j) = 0$ pour $j \neq i$). En divisant par $L_i(i)e^{ix} = e^{ix} \neq 0$, on obtient : $\alpha_i = 0$.

Ainsi : $\forall i \in [\![0, d]\!]$, $\alpha_i = 0$, ce qui prouve que la famille $(f_0, \ldots, f_d)$ est libre. Nous verrons une autre démonstration de sa liberté à l'exemple 4, avec un autre argument sur les racines d'un polynôme.

Nous donnons trois exercices avec des raisonnements très proches de celui de cet exemple. Ils utilisent tous le principe de la section *Indépendance linéaire* sur la multiplication du nombre d'équations.

Exercice 2. En s'inspirant de l'exemple précédent, montrer que la famille de fonctions $(x \mapsto \sin(kx))_{1 \leqslant k \leqslant d}$ est libre. Attention, c'est un peu plus subtil, à cause de la parité des puissances qui apparaîtront.

Exercice 3. Soit $n \in \mathbb{N}$. On veut montrer que la famille $((X+k)^n)_{0 \leqslant k \leqslant n}$ est libre. Soit $(\alpha_0, \ldots, \alpha_n) \in \mathbb{R}^{n+1}$ tel que : $\sum_{k=0}^{n} \alpha_k (X+k)^n = 0_{\mathbb{R}[X]}$.

1. Montrer : $\forall i \in [\![0, n]\!]$, $\sum_{k=0}^{n} \alpha_k \frac{n!}{(n-i)!}(X+k)^{n-i} = 0_{\mathbb{R}[X]}$, et en déduire : $\forall j \in [\![0, n]\!]$, $\sum_{k=0}^{n} \alpha_k k^j = 0$.
2. En déduire : $\forall P \in \mathbb{R}_n[X]$, $\sum_{k=0}^{n} \alpha_k P(k) = 0$, et conclure par des choix convenables de polynômes P.

Comme nous l'avons dit en fin de section 2, cette méthode doit s'affiner si les égalités à interpréter comme le lieu d'annulation d'un polynôme, concernent à chaque fois un polynôme différent. C'est le cas

lorsqu'on veut « fabriquer » un polynôme vérifiant plusieurs conditions du type $P(a_i) = b_i$, où les b_i ne sont pas tous égaux. Dans ce cas il faut faire preuve de plus de finesse, et recourir aux *polynômes d'interpolation de Lagrange*. Un polynôme qui convient est alors : $P = \sum_{i=1}^{n} b_i L_i$.

3 ✓ Montrer qu'un polynôme est nul

Nous avons décrit dans la section 1 ce qu'il se passe lorsqu'un polynôme P est annulé par k nombres $a_1, \dots, a_k$: il est divisible par $\prod_{i=1}^{k} (X - a_i)$. Or ce produit est de degré k, donc on doit avoir : $k \leqslant \deg(P)$, du moins si $P \neq 0_{\mathbb{R}[X]}$. On en déduit, par contraposée :

> Si P admet strictement plus de racines que son degré, alors P est le polynôme nul !

C'est en particulier le cas si P admet une infinité de racines (exemple : tous les réels d'un intervalle non réduit à un point, ou tous les entiers, etc.). C'est une situation très commode parce qu'elle ne nécessite pas de connaître le degré de P, qui est une donnée parfois manquante.

Ce raisonnement apparaît très souvent lorsqu'on veut démontrer l'injectivité d'une application linéaire définie sur $K[X]$, et en géométrie dans l'étude de produits scalaires sur $K[X]$. En fait, il est un peu partout : en effet, dès qu'une quantité vérifie des relations invoquant ses puissances et des sommes ou produits, c'est implicitement l'annulation d'une quantité polynomiale. Si cette annulation couvre tout un intervalle de $\mathbb{R}$ (par exemple), alors cet argument sur les racines assure que l'annulation vaut partout.

Il est utile de démontrer la nullité d'un polynôme dès qu'on a besoin de montrer la nullité de ses coefficients (exemple 4), ou dans les démonstrations de bijectivité d'une application linéaire (on a besoin en particulier de montrer que son noyau est trivial), mais aussi pour identifier les coefficients de deux polynômes (section 4) ou pour étendre une identité à un ensemble de valeurs plus grand que celui d'origine (section 5).

Exemple 4. Soit $d \in \mathbb{N} \setminus \{0\}$. Pour illustrer le paragraphe précédent, nous allons montrer que la famille $\left(f_0 : x \mapsto 1, f_1 : x \mapsto e^x, f_2 : x \mapsto e^{2x}, \dots, f_d : x \mapsto e^{dx}\right)$ est libre en passant par le lieu d'annulation d'un polynôme bien choisi. Soit $(a_0, \dots, a_{d+1}) \in \mathbb{R}^{d+1}$ tel que : $\sum_{i=0}^{d} a_i f_i = 0$. Alors : $\forall x \in \mathbb{R}$, $\sum_{i=0}^{d} a_i e^{ix} = 0$, ce qu'on peut réécrire, grâce aux propriétés de l'exponentielle :

$$\forall x \in \mathbb{R}, \quad \sum_{i=0}^{d} a_i \left(e^x\right)^i = 0.$$

On en déduit que le polynôme $P = \sum_{i=0}^{d} a_i X^i$ admet e^x pour racine pour tout $x \in \mathbb{R}$; or e^x prend une infinité de valeurs quand x parcourt $\mathbb{R}$ (vu que l'exponentielle tend vers $+\infty$ quand $x \to +\infty$), donc P admet une infinité de racines, ce qui n'est possible que si $P = 0_{\mathbb{R}[X]}$. Par conséquent tous ses coefficients sont nuls, c'est-à-dire : $\forall i \in [\![0, d]\!]$, $a_i = 0$, démontrant par là la liberté de la famille $(f_0, \dots, f_d)$.

Ce raisonnement se généralise à toute famille de puissances d'une fonction raisonnable.

Exercice 4. Soit $n \in \mathbb{N}$. Montrer que si I est un intervalle de $\mathbb{R}$ non réduit à un point, et si $f : I \to K$ est une application continue non constante, alors $\left(f^k\right)_{0 \leqslant k \leqslant n}$ est une famille libre de $\mathrm{C}^0(I, K)$ (ici f^k ne désigne pas $f \circ \cdots \circ f$, mais la puissance k^{e} de f, c'est-à-dire : $x \mapsto (f(x))^k$).

Exemple 5. (injectivité d'une application linéaire définie sur $K[X]$) Soit $(\alpha, \beta) \in K^2$ tel que $\alpha \neq \beta$. On veut montrer qu'il est possible de trouver un polynôme dont les valeurs en α et β, *ainsi que ses tangentes en ces nombres*, sont prescrites, c'est-à-dire : on veut montrer que pour tout

$(a,b,c,d) \in K^4$, il existe un polynôme $P \in K[X]$, unique si on le prend dans $K_3[X]$, tel que : $P(\alpha) = a$, $P(\beta) = b$, $P'(\alpha) = c$, et : $P'(\beta) = d$. Cela revient à démontrer que l'application :

$$f : \begin{cases} K_3[X] & \to & K^4 \\ P & \mapsto & (P(\alpha), P(\beta), P'(\alpha), P'(\beta)) \end{cases}$$

est bijective (surjective pour l'existence, injective pour l'unicité). Comme f est linéaire, et : $\dim(K_3[X]) = \dim(K^4) = 4$, il suffit de montrer qu'elle est injective pour avoir la bijectivité. Montrons-le en démontrant que $\ker(f)$ ne contient que le polynôme nul : soit $P \in K_3[X]$ tel que : $f(P) = (0,0,0,0)$. Alors : $P(\alpha) = P'(\alpha) = 0$, et : $P(\beta) = P'(\beta) = 0$. On en déduit que P admet α et β comme racines (au moins) doubles, ce qui fait quatre racines comptées avec multiplicités, pour un polynôme de degré au plus 3 : ce n'est possible que si $P = 0_{K_3[X]}$. D'où le résultat : $\ker(f) = \{0_{K_3[X]}\}$, donc f est injective, donc bijective par ce qui précède.

4 ✓ Montrer que deux polynômes sont égaux

On suppose dans cette section qu'on nous demande de montrer que $P = Q$, sachant qu'on a pour hypothèse : $\forall x \in I$, $\tilde{P}(x) = \tilde{Q}(x)$, où I est un certain ensemble de nombres. Commentons d'abord : 1° pourquoi cela ne va pas de soi, 2° à quoi cela peut bien servir.

1° Cela ne va pas de soi, puisque après tout, des fonctions peuvent bien coïncider par endroits : cela ne veut pas dire qu'elles sont égales partout. Par exemple la fonction partie entière vaut 0 sur $[0,1[$; cela ne veut pas dire pour autant qu'elle est nulle partout. Pour des applications polynomiales ce n'est pas différent, si l'ensemble I n'est pas assez contraignant ; après tout on a bien : $\forall x \in \{-1,0,1\}$, $x^4 = x^2$, mais cela ne prouve pas que $X^4 = X^2$ (clairement pas !).

2° L'égalité $P = Q$ est largement préférable à l'égalité : $\forall x \in I$, $\tilde{P}(x) = \tilde{Q}(x)$, pour plusieurs raisons. D'abord, parce que l'égalité $P = Q$ peut être évaluée partout (y compris en des objets non numériques comme des matrices), alors que $\tilde{P}(x) = \tilde{Q}(x)$ nécessite de prendre $x \in I$: c'est plus exigeant. On illustre cela dans la section suivante. Ensuite, parce qu'**il faut un polynôme, et non une application polynomiale, pour correctement invoquer la théorie des polynômes, et raisonner sur leur degré, leurs coefficients**, etc. Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux, mais ce n'est pas tout à fait le cas dans une égalité entre applications polynomiales : le contre-exemple en 1° le montre bien, ni le degré ni les coefficients ne sont les mêmes dans chaque membre de l'égalité. Évidemment, le « piège » est que l'égalité est valable en « trop peu » de x pour « contraindre » l'égalité des deux polynômes ; mais comment quantifier à partir de quel stade il y a « assez » de x ? Il faut être en mesure de passer aux polynômes, où il n'y a plus ambiguïté.

Ceci étant dit, expliquons comment montrer une implication du type : $\forall x \in I$, $\tilde{P}(x) = \tilde{Q}(x) \Rightarrow P = Q$. Ce n'est pas très différent du raisonnement de la section précédente :

- on réécrit l'égalité ainsi : $\forall x \in I$, $\tilde{R}(x) = 0$, où : $R = P - Q$;
- on en conclut que R admet pour racines tous les éléments x dans I ; si I contient strictement plus d'éléments que $\deg(R)$ (ce qui est automatique si I est infini), alors on en déduit $R = 0_{K[X]}$, c'est-à-dire : $P = Q$.

Exemple 6. Cherchons à quelle condition un polynôme $P \in \mathbb{R}[X]$ interpole la fonction carrée en tous les entiers, c'est-à-dire vérifie : $\forall k \in \mathbb{Z}$, $P(k) = k^2$ (faites bien attention à la différence dans la quantification avec l'exemple 2). Pour cela, on note que si P convient, alors le polynôme $P - X^2$ admet pour racines tous les entiers $k \in \mathbb{Z}$, donc une infinité de racines : ce n'est possible que si $P - X^2 = 0_{\mathbb{R}[X]}$, c'est-à-dire : $P = X^2$. Ainsi il n'existe qu'un seul polynôme interpolant la fonction carrée en tout entier.

Exemple 7. (raisonner sur le degré) On veut montrer qu'il n'existe pas de polynôme $P \in \mathbb{R}[X]$ interpolant la fonction inverse en les entiers naturels non nuls, c'est-à-dire tel que :

$$\forall k \in \mathbb{N} \setminus \{0\}, \quad P(k) = \frac{1}{k}.$$

L'idée informelle est : le membre de droite est de « degré -1 » (ce serait $\frac{1}{X}$, dans l'idée), alors que le degré d'un polynôme est un entier naturel. On a donc une absurdité en comparant les degrés. Mais le raisonnement n'est pas suffisamment rigoureux pour conclure à ce stade : d'abord, puisqu'il n'est question de degré que pour des polynômes (au programme de PSI), il faut se débarrasser du quotient pour se ramener à des quantités polynomiales. On y remédie en multipliant par k, et on obtient l'égalité équivalente : $\forall k \in \mathbb{N} \setminus \{0\}$, $kP(k) = 1$. Passons au deuxième problème : on ne peut identifier les degrés qu'entre deux polynômes, et là nous n'avons que des évaluations d'applications polynomiales en des entiers, donc ce n'est pas possible. Pour se convaincre que c'est un vrai problème, remarquez que l'égalité $kP(k) = 1$ est tout à fait possible si l'on est moins exigeant sur les valeurs de k prises : si l'on prend

$$P = -\frac{X^5}{720} + \frac{7X^4}{240} - \frac{35X^3}{144} + \frac{49X^2}{48} - \frac{203X}{90} + \frac{49}{20},$$

je vous laisse vérifier qu'on a $kP(k) = 1$ pour tout $k \in [\![1,6]\!]$ (comment ai-je trouvé un tel polynôme ?). Là, si on concluait à l'impossibilité en regardant les degrés, on serait en tort.

Ce n'est donc pas facultatif : il faut remonter aux polynômes pour parler de degré sans bizarrerie. Pour cela, on soustrait 1 à l'égalité ci-dessus, et obtient l'égalité équivalente :

$$\forall k \in \mathbb{N} \setminus \{0\}, \quad kP(k) - 1 = 0.$$

On en déduit que le polynôme $XP - 1$ s'annule en tous les entiers $k \in \mathbb{N} \setminus \{0\}$, et donc il admet une infinité de racines : ce n'est possible que si $XP - 1 = 0_{\mathbb{R}[X]}$. Mais alors on aurait : $XP = 1$, et une contradiction en comparant les degrés : en effet $\deg(X) + \deg(P) = \deg(1)$ donne : $1 + \deg(P) = 0$, c'est-à-dire : $\deg(P) = -1 \notin \mathbb{N}$: absurde.

Ainsi il n'existe pas de polynôme interpolant la fonction inverse en les entiers.

5 Étendre des identités

Un intérêt des polynômes, par rapport aux fonctions (qui ont un domaine de définition, en dehors duquel il est impossible de les évaluer), est qu'ils sont définis à l'aide d'une indéterminée X qui « peut être n'importe quoi », tant que c'est un objet mathématique pour lequel les sommes, produits et puissances ont un sens (ce qui, pour un élève de PSI, inclut à peu près tout sauf les vecteurs abstraits, qu'on ne peut pas multiplier ni élever à une puissance). C'est un principe que vous utilisez lorsqu'en algèbre linéaire, vous calculez des puissances de matrices *via* la division euclidienne de X^n par un polynôme annulateur. En peu de mots :

> Une identité polynomiale est **universellement** vraie.

Par identité polynomiale, j'entends une égalité de la forme $P = Q$, où P et Q sont des polynômes.

Ce principe est plus impressionnant si on le couple à une observation effectuée dans la section précédente : imaginons qu'on ait un sous-ensemble I de $\mathbb{R}$ ou $\mathbb{C}$ contenant strictement plus que $\deg(P)$ et $\deg(Q)$ éléments (prendre I un intervalle de $\mathbb{R}$ non réduit à un point par exemple). On a vu dans la section précédente comment démontrer l'implication : $\forall x \in I$, $\tilde{P}(x) = \tilde{Q}(x) \Rightarrow P = Q$. Alors que la première égalité ne pouvait être évaluée qu'en des éléments de I, la deuxième peut être évaluée en n'importe quoi, y compris des nombres complexes, des endomorphismes, des matrices (et bien d'autres choses encore que vous ne voyez pas en classes préparatoires), qui ne sont pas absolument pas des nombres.

En conclusion : si les évaluations de P et Q sont les mêmes en suffisamment de nombres, alors elles sont égales partout (c'est ce que j'appellerai le *principe de prolongement des identités polynomiales*).

Soit dit en passant, c'est la raison pour laquelle il était important de définir les polynômes autrement que comme des fonctions, et qu'on vous somme de distinguer polynômes et applications polynomiales : si l'on se contente de manipuler des applications polynomiales $x \mapsto \tilde{P}(x)$, elles sont

définies sur $\mathbb{R}$ ou $\mathbb{C}$, et par conséquent on ne peut pas remplacer x par un endomorphisme ou une matrice.

Ainsi les polynômes permettent d'étendre des identités : si vous montrez que leurs évaluations sont égales à une certaine quantité polynomiale en suffisamment de nombres réels ou complexes, alors vous en déduisez que l'égalité vaut partout. Il arrive néanmoins que, comme dans les sections précédentes, l'identité que vous souhaitez prolonger ne soit pas entre deux quantités polynomiales, à cause de la présence d'un quotient, d'une racine carrée, etc. Dans ce cas de figure, faites les opérations de circonstance pour qu'il n'y ait plus que des quantités polynomiales : multiplication par les dénominateurs, élévation au carré, ou que sais-je. Les deux exemples suivants l'illustreront.

Exemple 8. (étendre des entiers aux complexes) En parcourant le document de méthodologie sur la décomposition en éléments simples, vous avez peut-être été perturbés par la « quantification élastique » des égalités : tantôt on prend x réel, tantôt complexe. Fait-on ce qu'on veut ?

Un questionnement analogue peut se poser lorsqu'on veut calculer $\sum_{n=1}^{N} \frac{1}{n(n+1)}$ en décomposant en éléments simples le terme général. On cherche $(a,b) \in \mathbb{R}^2$ tel que : $\forall n \in \mathbb{N} \setminus \{0\}$, $\frac{1}{n(n+1)} = \frac{a}{n} + \frac{b}{n+1}$. Or, si l'on suit la méthode habituelle, on devrait prendre $n \to -1$ pour obtenir la valeur de b : impossible si n est un entier naturel non nul ! Pourquoi le raisonnement est-il possible pour autant ?

En fait, nous allons montrer sur ce cas particulier que si une décomposition en éléments simples est valable sur $\mathbb{N} \setminus \{0\}$, alors elle est valable en des réels voire des complexes, illustrant ainsi le principe de prolongement des identités polynomiales. Pour cela, nous remarquons que si : $\forall n \in \mathbb{N} \setminus \{0\}$, $\frac{1}{n(n+1)} = \frac{a}{n} + \frac{b}{n+1}$, alors en multipliant cette égalité par $n(n+1)$ pour éliminer les fractions, nous avons :

$$\forall n \in \mathbb{N} \setminus \{0\}, \quad 1 = a(n+1) + bn.$$

On en déduit que le polynôme $P = 1 - (a(X+1) + bX)$ admet tous les entiers $n \in \mathbb{N} \setminus \{0\}$ pour racines ; cela fait une infinité de racines, ce qui n'est possible que si $P = 0_{\mathbb{R}[X]}$. En particulier, si P est le polynôme nul, alors : $\forall z \in \mathbb{C}$, $\tilde{P}(z) = 0$, ce qui donne après réarrangement des termes : $\forall z \in \mathbb{C}$, $1 = a(z+1) + bz$. Après division par $z(z+1)$, ce qui est possible dès que $z \notin \{0, -1\}$: $\forall z \in \mathbb{C} \setminus \{0, -1\}$, $\frac{1}{z(z+1)} = \frac{a}{z} + \frac{b}{z+1}$. On peut expliciter a et b par la méthode classique désormais, puisque plus rien n'empêche de prendre $z \to 0$ ou $z \to -1$ si $z \in \mathbb{C} \setminus \{0, -1\}$.

Ce raisonnement vaudrait pour toute décomposition en éléments simples, et c'est pourquoi nous sommes parfois laxistes sur la quantification : que l'égalité soit vraie sur $\mathbb{N}$, $\mathbb{R}$ ou $\mathbb{C}$, on peut de toute façon l'étendre si besoin à tout nombre complexe grâce à un argument sur les racines d'un polynôme.

Exemple 9. (étendre des réels aux complexes et matrices) Soit $n \in \mathbb{N}$. On sait que pour tout $x \in \mathbb{R} \setminus \{1\}$, on a : $\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}$. En dérivant cette relation, on a donc :

$$\forall x \in \mathbb{R} \setminus \{1\}, \quad \sum_{k=1}^{n} k x^{k-1} = \frac{1 - x^{n+1}}{(1-x)^2} - \frac{(n+1)x^n}{1-x}.$$

Cette relation vaut *a priori* pour x réel (différent de 1). On peut se demander s'il est possible de l'étendre :

— en remplaçant x réel par z complexe (par exemple si l'on souhaite calculer $\sum_{k=1}^{n} k e^{ik\theta}$) ;

— en remplaçant x réel par une matrice A (et donc 1 par I_n pour que tout conserve un sens) suffisamment bien choisie pour que $(\mathrm{I}_n - A)^{-2}$ et $(\mathrm{I}_n - A)^{-1}$ existent.

Le miracle polynomial assure que oui : une identité polynomiale est pour ainsi dire universelle, or après multiplication par $(1-x)^2$ nous avons là une identité polynomiale. Mais formulons proprement les choses. On a, pour tout $x \in \mathbb{R} \setminus \{1\}$:

$$(1-x)^2 \sum_{k=1}^{n} k x^{k-1} - (1 - x^{n+1}) + (n+1)x^n(1-x) = 0,$$

ce qui prouve que le polynôme $P = (1-X)^2 \sum_{k=1}^{n} kX^{k-1} - (1-X^{n+1}) + (n+1)X^n(1-X)$ s'annule en tous les réels différents de 1. Cela lui fournit une infinité de racines, ce qui n'est possible que si $P = 0_{\mathbb{R}[X]}$. Ainsi on a **l'identité polynomiale** :

$$(1-X)^2 \sum_{k=1}^{n} kX^{k-1} - (1-X^{n+1}) + (n+1)X^n(1-X) = 0_{\mathbb{R}[X]}, \qquad (*)$$

et une identité entre polynômes peut s'évaluer en à peu près n'importe quoi. Par exemple en un nombre complexe $e^{i\theta}$ (avec $\theta \not\equiv 0 \bmod 2\pi$, choisi de sorte que $e^{i\theta} \neq 1$, pour qu'on puisse diviser par $1 - e^{i\theta}$), et on obtient alors :

$$\left(1-e^{i\theta}\right)^2 \sum_{k=1}^{n} k\left(e^{i\theta}\right)^{k-1} - (1-\left(e^{i\theta}\right)^{n+1}) + (n+1)\left(e^{i\theta}\right)^n \left(1-e^{i\theta}\right) = 0,$$

puis, après réarrangement des termes et division par $\left(1-e^{i\theta}\right)^2 \neq 0$:

$$\sum_{k=1}^{n} ke^{i(k-1)\theta} = \frac{1-e^{i(n+1)\theta}}{(1-e^{i\theta})^2} - \frac{(n+1)e^{in\theta}}{1-e^{i\theta}}.$$

Mais on peut aussi évaluer l'identité polynomiale $(*)$ en une matrice A, qu'on va choisir telle que $A^n = 0_{\mathrm{M}_n(K)}$ pour simplifier l'expression (c'est alors une matrice *nilpotente* ; $A = \begin{pmatrix} 0 & * & * \\ \vdots & \ddots & * \\ 0 & \cdots & 0 \end{pmatrix}$ conviendrait par exemple). On obtient sous cette hypothèse :

$$(\mathrm{I}_n - A)^2 \sum_{k=1}^{n} kA^{k-1} = \mathrm{I}_n,$$

ce qui démontre en passant que si $A^n = 0_{\mathrm{M}_n(K)}$, alors $(\mathrm{I}_n - A)^2$ est inversible, et son inverse est $\sum_{k=1}^{n} kA^{k-1}$: chose loin d'être évidente !

Nous donnons une application du prolongement des identités polynomiales à un exercice classique de réduction : on peut expliciter les projecteurs sur un sous-espace propre d'un endomorphisme diagonalisable (parallèlement aux autres sous-espaces propres) grâce aux polynômes d'interpolation de Lagrange.

Exercice 5. Soit f un endomorphisme *diagonalisable*, dont on note $\lambda_1, \ldots, \lambda_k$ les valeurs propres. Soient $L_1, \ldots, L_k$ les polynômes interpolateurs de Lagrange en les $\lambda_1, \ldots, \lambda_k$.

1. Rappeler pourquoi on a : $\sum_{i=1}^{k} L_i = 1$, et en déduire : $\forall \vec{x} \in E$, $\vec{x} = \sum_{i=1}^{k} L_i(f)(\vec{x})$.
2. (a) Rappeler pourquoi le polynôme $P = \prod_{i=1}^{k} (X - \lambda_i)$ annule f.
   (b) L'utiliser pour en déduire que pour tout $(i,j) \in [\![1,k]\!]^2$ tel que $i \neq j$, on a : $L_i(f) \circ L_j(f) = 0$.
   (c) Utiliser les questions 1 et 2.(b) pour en déduire : $\forall j \in [\![1,k]\!]$, $L_j(f) \circ L_j(f) = L_j(f)$. Ainsi les polynômes d'interpolation de Lagrange en f sont des projecteurs.
3. Montrer, pour tout $i \in [\![1,k]\!]$, que $(f - \lambda_i \mathrm{Id}_E) \circ L_i(f)$ est égal à $P(f)$ à une constante multiplicative près, et en déduire : $\forall \vec{x} \in E$, $\forall i \in [\![1,k]\!]$, $L_i(f)(\vec{x}) \in \ker(f - \lambda_i \mathrm{Id}_E)$.
4. Conclure que pour tout $i \in [\![1,k]\!]$, le projecteur $L_i(f)$ est celui sur $\ker(f - \lambda_i \mathrm{Id}_E)$ parallèlement à $\bigoplus_{\substack{j=1 \\ j \neq i}}^{k} \ker(f - \lambda_j \mathrm{Id}_E)$, et qu'on a : $f = \sum_{i=1}^{k} \lambda_i L_i(f)$.

L'application suivante montre que grâce au prolongement des identités, on peut extraire des « racines carrées de matrices » *via* l'approximation de la racine carrée réelle par une application polynomiale (la partie régulière de son développement limité). Extension inattendue !

Exercice 6. Soit $p \in \mathbb{N}$.

1. À l'aide du développement limité de $x \mapsto \sqrt{1+x}$ en 0 à l'ordre p, montrer l'existence d'un polynôme $P \in \mathbb{R}[X]$, que l'on sait expliciter si besoin, tel que : $1 + x = (P(x))^2 + \underset{x\to 0}{o}(x^p)$.
2. Effectuer la division euclidienne de $1 + X - P^2$ par X^p, et utiliser la question précédente, pour montrer l'existence de $Q \in \mathbb{R}[X]$ tel que : $1 + X = P^2 + X^p Q$.
3. **Application.** On prend $p = 2$ dans cette question. Montrer que $P = 1 + \dfrac{X}{2}$ convient dans ce cas, et en déduire une matrice $B \in \mathrm{M}_2(\mathbb{C})$ telle que : $B^2 = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} = \mathrm{I}_2 + \begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix}$.
4. Adapter le raisonnement pour montrer que pour tout $k \in \mathbb{N} \setminus \{0\}$ et toute matrice $A \in \mathrm{M}_p(\mathbb{C})$ telle que : $A^p = 0_{\mathrm{M}_p(\mathbb{C})}$, il existe $B \in \mathrm{M}_p(\mathbb{C})$ telle que : $\mathrm{I}_p + A = B^k$ (« toute matrice unipotente admet une racine k^{e} »).

Il existe un phénomène analogue dans le cas des séries entières, qu'on appelle le *principe du prolongement analytique* : voir la section 5 du document *Méthodes* du chapitre sur les séries entières.

Table des matières