Chapitre 12 : Polynômes

PTSI B Lycée Eiffel

7 février 2014

Monsieur et Madame Ôme ont une fille, comment s'appelle-t-elle ?

Il faut vraiment que je donne la réponse ?

Il s'embrouillait dans les polynômes, se disculpa
le professeur de mathématiques, et quand un élève
s'embrouille dans les polynômes, que peut-on faire ?

Antonio Lobo Antunes.

Introduction

Avant de s'attaquer vraiment à l'algèbre linéaire, ce chapître servira d'introduction par l'exemple aux concepts plus généraux développés ensuite dans toute leur généralité sur les espaces vectoriels. Les polynômes constituent en effet un excellent exemple d'objet mathématique formel, mais avec lequel on peut faire des calculs, par le biais d'opérations simples comme la somme, le produit ou la composition. C'est ce genre de notions (opérations « utiles » sur un ensemble) que nous essaierons de généraliser ensuite. Ce chapître sera également l'occasion de croiser pour la première fois une formule d'importance capitale en analyse, et que nous retrouverons sous d'autres formes à plusieurs reprises ensuite : la formule de Taylor.

Objectifs du chapitre :

- savoir factoriser ou effectuer une division euclidienne sur des polynômes à coefficients réels ou complexes.
- comprendre ce que signifie la formule de Taylor d'un point de vue analytique.

1 L'ensemble $\mathbb{K}[X]$

Dans toute ce chapître, $\mathbb{K}$ désigne soit l'ensemble $\mathbb{R}$ des nombres réels ou l'ensemble $\mathbb{C}$ des nombres complexes. Pour les plus curieux, toute la construction effectuée ici peut être généralisée à un corps $\mathbb{K}$ quelconque, c'est-à-dire à un ensemble munis de deux opérations de somme et de produit « sympathiques » (associatives, commutatives, distributibe l'une par rapport à l'autre, admettant chacune un élément neutre et telles que tout élément ait un opposé et un inverse, sauf 0 en ce qui concerne l'inverse).

Définition 1. Un **polynôme à coefficients dans** $\mathbb{K}$ est un objet mathématique formel s'écrivant $P = \sum_{k=0}^{k=n} a_k X_k$, où $(a_0, a_1, \ldots, a_n) \in \mathbb{K}^{n+1}$, et X est une indéterminée destinée à être remplacée par n'importe quel objet pour lequel le calcul de P peut avoir un sens (donc en gros des éléments qu'on sait élever à une certaine puissance et multiplier par des éléments de $\mathbb{K}$, par exemple des matrices, des suites ou des fonctions).

Définition 2. On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$.

Définition 3. Soit $P = \sum_{k=0}^{k=n} a_k X^k$ un polynôme, avec $a_n \neq 0$. Les nombres a_k sont appelés **coefficients** du polynôme P, l'entier n **degré** de P (souvent noté $d^\circ(P)$), le coefficient correspondant a_n est le **coefficient dominant** de P. Si ce coefficient est égal à 1, on dit que P est un polynôme **unitaire**.

Remarque 1. Par convention, le polynôme nul a pour degré $-\infty$. C'est relativement cohérent avec les propriétés énoncées ci-dessous.

Définition 4. Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_p X^p$ deux polynômes dans $\mathbb{K}[X]$, leur **somme** est le polynôme $P + Q = \sum_{k=0}^{\max(n,p)} (a_k + b_k) X^k$.

Proposition 1. Cette somme de polynômes est associative ($(P+Q)+R = P+(Q+R)$), commutative ($P + Q = Q + P$), admet pour élément neutre le polynôme nul (noté 0) dont tous les coefficients sont nuls, et tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ admet un opposé noté $-P$ défini par $-P = \sum_{k=0}^{n} (-a_k) X^k$, et vérifiant $P + (-P) = 0$.

Démonstration. L'associativité découle trivialement de celle de l'addition des réels (ou des complexes) en regardant ce qui se passe degré par degré. De même, la commutativité est évidente. À vrai dire, le reste aussi ! □

Définition 5. Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_p X^p$ deux polynômes dans $\mathbb{K}[X]$, leur **produit** est le polynôme $PQ = \sum_{k=0}^{n+p} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$.

Proposition 2. Ce produit de polynômes est associatif, commutatif, admet pour élément neutre le polynôme constant 1. De plus, le produit est distributif par rapport à la somme : $P(Q + R) = PQ + PR$.

Démonstration. Ces résultats sont nettement moins évidents à prouver que pour la somme. La commutativité s'obtient assez facilement en effectuant le changement d'indice $j = k - i$ dans la somme intérieure de la définition du produit. La distributivité est également assez facile en découpant simplement la somme définissant $P(Q + R)$ en deux morceaux. Le fait que 1 soit élément neutre est facile. Par contre, l'associativité est franchement pénible, puisqu'il faut des triples sommes pour décrire le produit $P(QR)$. Contentons-nous d'écrire son coefficient de degré k (en notant a_i, b_j et c_p les coefficients respectifs des polynômes P, Q et R) : il vaut $\sum_{i=0}^{p} a_i \sum_{j=0}^{k-i} b_j c_{k-i-j}$. On peut l'écrire plus simplement sous la forme $\sum_{i+j+p=k} a_i b_j c_k$. Cette formule est complètement symétrique par rapport

aux trois polynômes, on obtiendra exactement la même pour $(PQ)R$, ce qui prouve l'associativité du produit. □

Remarque 2. Les propriétés énoncées pour la somme de polynômes et pour le cas particulier du produit que sont les produits de polynômes par des constantes font de $\mathbb{K}[X]$ ce qu'on appelle un espace vectoriel sur $\mathbb{K}$. Vous aurez bien sûr droit à une définition complète (et affreuse) dans un chapître ultérieur, mais l'idée est là : un produit par des constantes et une addition qui vérifient quelques propriétés élémentaires naturelles.

Proposition 3. Soient P et Q deux polynômes, alors $d^\circ(P+Q) \leqslant \max(d^\circ(P), d^\circ(Q))$, et $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$.

Démonstration. Cela découle immédiatement des définitions données des deux opérations. L'inagalité peut être stricte pour le degré de la somme, dans le cas où P et Q sont de même degré mais ont un coefficient dominant opposé. Par contre, c'est toujours une égalité pour le produit, le coefficient dominant du produit étant le produit des coefficients dominants de P et Q. □

Remarque 3. Les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants (non nuls).

Définition 6. Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Remarque 4. Ces ensembles $K_n[X]$ sont stables par somme (contrairement à l'ensemble des polynômes de degré exactement n), ce qui est une des conditions pour en faire des sous-espaces vectoriels de $\mathbb{K}[X]$.

Définition 7. Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes, le **polynôme composé** de P et Q est le polynôme $P \circ Q = \sum_{k=0}^{n} a_k Q^k$.

Exemple : Si $P = X^2 + 1$ et $Q = 2X + 3$, alors $P \circ Q = (2X+3)^2 + 1 = 4X^2 + 12X + 10$, alors que $Q \circ P = 2(X^2+1) + 3 = 2X^2 + 5$.

Proposition 4. Si P et Q sont deux polynômes, $d^\circ(P \circ Q) = d^\circ(P) \times d^\circ(Q)$.

Démonstration. En effet, $P \circ Q = \sum_{k=0}^{n} a_k (\sum_{i=0}^{p} b_i X^i)^k$, dont le terme dominant vaut (si on développe tout brutalement à coups de formules du binôme de Newton) $a_n b_p^n X^{in}$. □

2 Arithmétique dans $\mathbb{K}[X]$.

2.1 Division euclidienne.

Définition 8. Un polynôme P est **divisible** par un polynôme Q s'il existe un troisième polonôme A tel que $P = AR$.

Remarque 5. Cette relation n'est pas une relation d'ordre sur $\mathbb{K}[X]$, elle est réflexive et transitive mais pas antisymétrique. Deux polynômes qui se divisent l'un l'autre sont simplement égaux à une constante multiplicative près. Dans ce cas, on dit que les deux polynômes sont **associés**.

Théorème 1. Division euclidienne dans $\mathbb{K}[X]$.
Soient $A, B \in \mathbb{K}[X]^2$, alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $d^\circ(R) < d^\circ(B)$. Le polynôme Q est appelé **quotient** de la division de A par B, et le polynôme R **reste** de cette même division.

Démonstration. La preuve de l'existence de la division peut se faire par récurrence sur le degré de A, le polynôme B restant fixé. L'existencce est triviale si $d^\circ(A) < d^\circ(B)$ puisqu'on peut écrire $A = 0B + A$, ce qui sert d'initialisation. Supposons désormais l'existence de la division prouvée pour tout polynôme de degré n, et choisissons A un polynôme de degré $n+1$. Notons a_nX^{n+1} son terme dominant, et b_pX^p celui de B, alors $C = A - \dfrac{a_n}{b_p}X^{n+1-p}B$ est un polynôme de degré n (en effet, on a soustrait à A un polynôme de même degré et de même coefficient dominant. Par hypothèse de récurrence, il existe donc des polynômes Q et R tels que $C = BQ + R$, avec $d^\circ(R) < d^\circ(B)$. Mais alors $A = \left(Q + \dfrac{a_n}{b_p}X^{n+1-p}\right)B + R$, et comme R n'a pas changé de degré, on vient d'écrire une division euclidienne de A par B.
Pour l'unicité, on suppose évidemment qu'il y a deux couples possibles : $BQ + R = BQ' + R'$, alors $B(Q - Q') = R - R'$, avec par hypothèse et règles de calculs sur le degré d'une somme $d^\circ(R - R') < d^\circ(B)$. Or, $d^\circ(B(Q - Q')) \geqslant d^\circ(B)$, sauf si $Q - Q' = 0$, soit $Q = Q'$. On en déduit que $R - R' = 0$, donc les deux couples sont égaux. □

Exemple : Pour effectuer en pratique une division euclidienne de polynômes, on procède comme pour les entiers, par exemple pour diviser $X^4 - 3X^3 + 5X^2 + X - 3$ par $X^2 - 2X + 1$:

$$\begin{array}{rrrrrrrrrr|l}
 & X^4 & - & 3X^3 & + & 5X^2 & + & X & - & 3 & X^2-2X+1 \\
\hline
- & (X^4 & - & 2X^3 & + & X^2) & & & & & X^2-X+2 \\
 & & - & X^3 & + & 4X^2 & + & X & - & 3 & \\
 & & - & (-X^3 & + & 2X^2 & - & X) & & & \\
 & & & & & 2X^2 & + & 2X & - & 3 & \\
 & & & & - & (2X^2 & - & 4X & + & 2) & \\
 & & & & & & & 6X & - & 5 &
\end{array}$$

Conclusion : $X^4 - 3X^3 + 5X^2 + X - 3 = (X^2 - X + 2)(X^2 - 2X + 1) + 6X - 5$. Cette méthode de calcul est une alternative à l'identification lorsqu'on cherche à factoriser un polynôme, par exemple après en avoir trouvé une racine évidente.

2.2 Racines et factorisation.

Définition 9. Soit $P \in \mathbb{K}[X]$ et $x \in \mathbb{K}$. On dit que x est une **racine** du polynôme P si $P(x) = 0$.

Remarque 6. On identifie ici le polynôme et la fonction polynômiale associée, comme ce sera le cas dans toute ce paragraphe. Il y a tout de même une certaine ambiguïté sur le terme racine dans le cas d'un polynôme à coefficients réels, qui peut également être vu comme un cas particulier de polynôme à coefficients complexes. Si le besoin s'en fait sortir, on explicitera en parlant de racines réelles ou de racines complexes du polynôme.

Proposition 5. Un réel a est racine du polynôme P si et seulement si $X - a$ divise P.

Démonstration. C'est une conséquence de la division euclidienne. Si on effectue la division de P par $X-a$, on sait que le reste sera de degré strictement inférieur à celui de $X-a$, donc sera une constante. Autrement dit, $\exists k \in \mathbb{R}$, $P = Q(X - a) + k$. On a donc $P(a) = 0 \Leftrightarrow Q(a)(a - a) + k = 0 \Leftrightarrow k = 0$. Autrement dit, a est une racine de P lorsque le reste de la division de P par $X - a$ est nul, donc quand P est divisible par $X - a$. □

Exemple : on a déjà fréquemment utilisé cette propriété pour factoriser des polynômes de degré 3 possédant une récine « évidente ». Soit par exemple $P = 2X^3 - 3X^2 + 5X - 4$. On constate que 1 est racine évidente de P : $P(1) = 2 - 3 + 5 - 4 = 0$, donc P est factorisable par $X - 1$: $P = (X - 1)(aX^2 + bX + c) = aX^3 + (b - a)X^2 + (c - b)X - c$. Par identification, on obtient $a = 2$; $b - a = -3$; $c - b = 5$ et $-c = -4$, donc $a = 2$; $b = -1$ et $c = 4$, soit $P = (X - 1)(2X^2 - X + 4)$. Ce dernier facteur ayant un discriminant négatif, P n'admet pas d'autre racine réelle que 1.

Corollaire 1. Un polynôme admet a_1, a_2, …, a_k comme racines distinctes si et seulement si il est divisible par $\prod_{i=1}^{k}(X - a_i)$.

Démonstration. On peut procéder par récurrence sur le nombre de racines distinctes. L'initialisation correspond à la propriété précédente. Si on suppose qu'on polynôme P à k racines distinctes est toujours factorisable comme décrit, en ajoutant une racine a_{k+1}, on pourra commencer par écrire $P = \prod_{i=1}^{k}(X - a_i) \times Q$, et comme $P(a_{i+1}) = 0$, on a nécessairement $Q(a_{i+1}) = 0$ (en effet, les facteurs précédents $a_{i+1} - a_i$ ne peuvent s'annuler puisque les racines sont supposées distinctes). En appliquant à nouveau notre propriété, on peut donc écrire $Q = (X - a_{k+1})R$, ce qui donne la factorisation souhaitée pour P, et achève la récurrence. □

Corollaire 2. Un polynôme de degré n admet au maximum n racines distinctes.

Démonstration. En effet, s'il en avait plus, on pourrait l'écrire sous la forme $\prod_{k=1}^{n+1}(X - a_i) \times Q$, qui est de degré au moins $n + 1$. Il y a là une contradiction flagrante. □

Corollaire 3. Un polynôme admettant une infinité de racines est nécessairement le polynôme nul.

Démonstration. En effet, par contraposée, un polynôme non nul a un certain degré n, et ne peut donc pas avoir plus de n racines. □

Corollaire 4. Principe d'identification des coefficients.
Si deux polynômes P et Q correspondent à des fonctions polynômiales identiques, alors $P = Q$.

Démonstration. Dans ce cas, $P - Q$ est un polynôme admettant tous les réels (ou tous les complexes) comme racines, ce qui en fait une grosse infinité, donc $P - Q = 0$. C'est bien ce principe qu'on utilise pour identifier les coefficients de deux polynômes correspondant à des expressions polynômiales égales. □

Définition 10. Soit P un polynôme et a une racine de P. On dit que a est une racine **d'ordre de multiplicité** $k \in \mathbb{N}^*$ si $(X - a)^k$ divise P, mais $(X - a)^{k+1}$ ne divise pas P.

Définition 11. Soit $P = \sum_{k=0}^{k=n} a_k X^k \in \mathbb{K}[X]$. Le **polynôme dérivé de** P est le polynôme $P' = \sum_{k=1}^{k=n} k a_k X^{k-1}$. On notera également P'' le polynôme de dérivé de P', et $P^{(n)}$ le polynôme dérivé n fois du polynôme P.

Remarque 7. Cette dérivation, bien que définie de façon formelle, coïncide évidemment avec la dérivation usuelle sur les fonctions polynômiales, et de ce fait vérifie toutes les formules de dérivation usuelle. En particulier celle rappelée ci-dessous :

Proposition 6. Formule de Leibniz.

Soient P et Q deux polynômes, alors $\forall n \in \mathbb{N}$, $(PQ)^{(n)} = \sum_{k=0}^{k=n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Proposition 7. Une racine a est d'ordre de multiplicité k pour P si et seulement si $P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Démonstration. Une façon de prouver ce résultat est de prouver le lemme suivant : si a est racine d'ordre k de P alors a est racine d'ordre $k-1$ de P'. En effet, si $P = (X_a)^k Q$, avec $Q(a) \neq 0$ alors $P' = k(X-a)^{k-1}Q + (X-a)^k Q' = (X-a)^{k-1}(kQ + (X-a)Q')$, avec $kQ(a) + (a-a)Q'(a) = kQ(a) \neq 0$. Par une récurrence facile, une racine d'ordre k sera donc racine de tous les polynômes dérivés jusqu'au $k-1$-ème, mais pas du k-ème. □

Remarque 8. On emploie souvent plus simplement le terme d'ordre ou celui de multiplicité à la place d'ordre de multiplicité.

Exemple : Considérons le polynôme $P = X^4 - 2X^3 - 19X^2 + 68X - 60$ et constatons ensemble que 2 est une racine double de P. En effet, on a $P(2) = 16 - 2\times 8 - 19\times 4 + 68\times 2 - 60 = 16 - 16 - 76 + 136 - 60 = 0$; de plus, $P' = 4X^3 - 6X^2 - 38X + 68$, donc $P'(2) = 4\times 8 - 6\times 4 - 38\times 2 + 68 = 32 - 24 - 76 + 68 = 0$. on peut en déduire, via la proposition précédente, que P est factorisable par $(X-2)^2$. Effectuons une petite division euclidienne pour obtenir cette factorisation :

$$\begin{array}{rcccccccc|l}
X^4 & - & 2X^3 & - & 19X^2 & + & 68X & - & 60 & \dfrac{X^2 - 4X + 4}{X^2 + 2X - 15} \\
- \ (X^4 & - & 4X^3 & + & 4X^2) & & & & & \\
 & & 2X^3 & - & 23X^2 & + & 68X & - & 60 & \\
 & - & (2X^3 & - & 8X^2 & + & 8X) & & & \\
 & & & - & 15X^2 & + & 60X & - & 60 & \\
 & & & - & (-15X^2 & + & 60X & - & 60) & \\
 & & & & & & & & 0 &
\end{array}$$

On a donc $P(X) = (X-2)^2(X^2+2X-15)$. Le deuxième facteur a pour discriminant $\Delta = 4+60 = 64$, et admet deux racines réelles $x_1 = \dfrac{-2-8}{2} = -5$ et $x_2 = \dfrac{-2+8}{2} = 3$. On peut donc factoriser P sous la forme $P(X) = (X-2)^2(X-3)(X+5)$. On ne risque pas de factoriser plus puisqu'il ne reste que des facteurs de degré 1.

Remarque 9. Un polynôme de degré n ne peut admettre plus de n racines comptées avec multiplicité. Ainsi, un polynôme de degré 5 admettant une racine triple ne peut plus admettre que deux autres racines.

Définition 12. Un polynôme P est **scindé** s'il peut s'écrire comme produit de polynômes de degré 1 (autrement s'il a un nombre de racines égal à son degré). Il est **scindé à racines simples** si de plus toutes ses racines sont distinctes.

Théorème 2. Théorème de d'Alembert-Gauss.
Tout polynôme dans $\mathbb{K}[X]$ est scindé.

Démonstration. Ce résultat fondamental a déjà été croisé dans le chapître sur les nombres complexes. Nous n'avons toujours pas les moyens de le démontrer maintenant. □

Exemple : Le polynôme $X^4 - 1$ se factorise dans $\mathbb{C}[X]$ sous la forme $X^4 - 1 = (X-1)(X+1)(X-i)(X+i)$.

Théorème 3. Tout polynôme $P \in \mathbb{R}[X]$ peut se factoriser sous la forme $P = \alpha(X-a_1)\dots(X-a_k)Q_1\dots Q_p$, où α est le coefficient dominant de P, les a_i sont les racines réelles du polynôme P, et les polynômes Q_i sont des polynômes de degré 2 à discriminant strictement négatif.

Démonstration. Puisqu'on peut identifier $\mathbb{R}$ à un sous-corps de $\mathbb{C}$, le polynôme P peut être vu comme un élément de $\mathbb{C}[X]$ et donc s'écrire, d'après le théorème précédent, sous la forme $P = \prod_{j=1}^{d^\circ(P)} (X - \alpha_i)$, où les α_i sont les racines complexes de P. Parmi tous ces facteurs, on peut déjà isoler tous ceux qui correspondent à des racines réelles, qui donneront les premiers termes dans la factorisation annoncée. Reste à savoir quoi faire des racines complexes. Commençons par constater que, si z est

racine complexe de P, alors $\overline{z}$ également. En effet, $P(\overline{z}) = \sum_{k=1}^{n} a_k \overline{z}^k = \sum_{k=1}^{n} \overline{a_k z^k} = \overline{P(z)}$, puisque les coefficients a_k sont réels et donc égaux à leur conjugué. Si $P(z) = 0$, on aura également $\overline{P(z)} = 0$, donc $P(\overline{z}) = 0$. De plus, la multiplicité de z sera toujours la même que celle de $\overline{z}$ puisque le raisonnement précédent peut s'appliquer à l'identique aux polynômes dérivés successifs de P. On peut donc regrouper tous les termes faisant intervenir des racines complexes sous la forme (quitte à répéter plusieurs fois chaque racine et chaque conjugué) $(X - z_1)(x - \overline{z_1}) \dots (X - z_p)(X - \overline{z_p})$. Reste à constater que $(X - z_i)(X - \overline{z_i}) = X^2 - (z_i + \overline{z_i})X + z_i\overline{z_i} = X^2 - 2\text{Re}\ (z_i) + |z_i|^2$ est un polynôme de degré 2 à coefficients réels, et à discriminant négatif puisque ses racines sont complexes. La factorisation annoncée en découle. □

Définition 13. Un polynôme P est **irréductible** s'il ne peut pas se décomposer comme produit de deux polynômes de degré strictement inférieur au sien. Autrement dit, les seuls diviseurs d'un polynôme irréductibles sont ses polynômes associés et les polynômes constants.

Remarque 10. Par convention, on décrète que les polynômes constants ne sont pas irréductibles.

Théorème 4. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Théorème 5. Tout polynôme $P \in \mathbb{K}[X]$ s'écrit comme produit de facteurs irréductibles, et ce produit est unique à l'ordre des facteurs et au remplacement de certains polynômes par des polynômes associés près.

Démonstration. Ces derniers théorèmes ne sont que des façons légèrement différentes d'énoncer la factorisation des polynômes vue un peu plus haut. L'unicité de la décomposition en produit d'irréductibles est admise. □

2.3 Relations coefficients-racines.

Proposition 8. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, et α_1, α_2, …, α_n ses racines (éventuellement répétées plusieurs fois). On a alors les relations suivantes entre les coefficients et les racines de P :

- $\sum_{k=1}^{k=n} \alpha_i = -\frac{a_{n-1}}{a_n}$
- $\sum_{1 \leqslant i < j \leqslant n} \alpha_i \alpha_j = \frac{a_{n-2}}{a_n}$
- …
- $\sum_{1 \leqslant i_1 < i_2 < \dots < i_p \leqslant n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_p} = (-1)^p \frac{a_{n-p}}{a_n}$
- …
- $\prod_{k=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$

Démonstration. Il suffit d'identifier la forme développée du polynôme et sa forme factorisée. On sait que $P = a_n(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$. Si on développe brutalement ce produit, le terme dominant sera $a_n X^n$ (heureusement !), le terme de degré $n-1$ est obtenu dans le développement en piochant des X dans $n-1$ parenthèses et un coefficient dans la dernière, ce qui donne $a_n(-\alpha_1 X^{n-1} - \alpha_2 X^{n-1} - \dots - \alpha_n X^{n-1})$, qu'on identifie à $a_{n-1}X^{n-1}$ pour obtenir la première formule annoncée. Les autres sont obtenues de la même façon, les termes en X^{n-p} étant obtenus en prenant au choix p racines dans p parenthèses et $n-p$ X dans les autres, ce qui donne un terme en $(-1)^p \alpha_{i_1} \dots \alpha_{i_p} X^{n-p}$. Le terme constant est obtenu en prenant les racines dans toutes les parenthèses, il est égal à $a_n \times (-1)^n \prod_{k=1}^{n} \alpha_i$. □

Exemple : Pour un polynôme de degré 4 ayant pour racines a, b, c et d, les formules deviennent $a+b+c+d=-\dfrac{a_3}{a_4}$; $ab+ac+ad+bc+bd+cd=\dfrac{a_2}{a_4}$; $abc+abd+acd+bcd=-\dfrac{a_1}{a_4}$ et $abcd=\dfrac{a_0}{a_4}$.

Exemple : On cherche à factoriser le polynôme $4X^3-4X^2-15X+18$, sachant qu'un ami nous a glissé un indice : il possède une racine double. deux méthodes sont possibles pour celà.

Première méthode : Puisqu'il y a une racine double, celle-ci est également racine de P'. Or, $P'=12X^2-8X-15=4\left(3X^2-2X-\dfrac{15}{4}\right)$. Ce trinôme a pour discriminant $\Delta=4+3\times 15=49$, et admet pour racines $X_1=\dfrac{2+7}{6}=\dfrac{3}{2}$ et $X_2=\dfrac{2-7}{6}=-\dfrac{5}{6}$. Vérifions si X_1 est racine de P : $4\times\dfrac{27}{8}-4\times\dfrac{9}{4}-\dfrac{45}{2}+18=\dfrac{27}{2}-\dfrac{45}{2}+9=0$, donc $\dfrac{3}{2}$ est la racine double recherchée. Inutile de vérifier si $\dfrac{5}{6}$ est aussi racine double, un polynôme de degré 3 ne peut pas avoir deux racines doubles. Pour déterminer la dernière racine, on peut effectuer une division euclidienne ou plus simplement utiliser le fait que le produit des trois racines sera égal à $-\dfrac{18}{4}$. Comme ce produit vaut, en notant α la dernière racine, $\left(\dfrac{3}{2}\right)\times\alpha=\dfrac{9}{4}\alpha$, on en déduit que $\alpha=-2$, et $P=4\left(X-\dfrac{3}{2}\right)^2(X+2)$.

Deuxième méthode : On utilise directement les relations coefficients-racines. En notant a la racine double et b la troisième racine de P, on aura le système $\begin{cases} 2a+b &= 1\\ a^2+2ab &= -\dfrac{15}{4}\\ a^2b &= -\dfrac{9}{2}\end{cases}$ En substituant $b=1-2a$ dans la deuxième équation, on trouve $a^2+2a(1-2a)=-\dfrac{15}{4}$, soit $-3a^2+2a+\dfrac{15}{4}=0$. Tiens, comme c'est curieux, c'est la même équation que plus haut. Pour déterminer si les deux solutions trouvées sont valables, on vérifie que la troisième équation du système fonctionne avec les valeurs obtenues. Si $a=-\frac{5}{6}$, on trouive $b=1-2a=\dfrac{8}{3}$, d'où $a^2b=\dfrac{25}{36}\times\dfrac{8}{3}=\dfrac{50}{27}$, ce qui assez différent de $-\dfrac{9}{2}$. Par contre, si $a=\dfrac{3}{2}$, $b=1-2a=-2$, et $a^2b=\dfrac{9}{4}\times(-2)=-\dfrac{9}{2}$, là ça marche. La conclusion est la même que ci-dessus.

3 Formule de Taylor sur les polynômes.

Les formules de Taylor sont un outil complètement fondamental en analyse, permettant d'effectuer les calculs de développements limités qui vous permettront enfin d'ici quelques semaines de voir sous un jour nouveau les calculs de limites. Le principe en est simple : généraliser la notion de droite tangente à une courbe en approchant le plus possible une courbe donnée (en un point donné) par la courbe d'une fonction polynômiale. rien d'étonnant donc à en trouver un premier énoncé dans ce chapître consacré aux polynômes. Ici, pas question d'approximation, puisqu'un polynôme est évidemment simplement égal à lui-même, mais l'idée est de comprendre qu'il existe plusieurs façons différentes de décrire un même polynôme. L'ensemble $\mathbb{R}_n[X]$ étant ce qu'on appelle un espace vectoriel de dimension $n+1$ (cf plus loin), on peut décrire un polynôme de degré n en donnant $n+1$ réels. On peut le faire d'au moins trois façons :

- donner les coefficients du polynôme. C'est la façon la plus classique de procéder, mais l'information donnée est finalement assez peu commode à exploiter autrement que très globalement (que signifie le fait qu'un polynôme de degré 8 a un coefficient de degré 3 égal à 5 ? Essentiellement rien).
- donner les valeurs du polynôme en $n+1$ réels distincts. Nous allons détailler plus bas cette méthode qui donne une information très concrète mais éparpillée à $n+1$ endroits différents.

- la troisième méthode que nous allons voir concentre réellement toute l'information au même endroit, puisque la formule de Taylor reconstitue le polynôme à partir des valeurs de ses différentes dérivées en un même réel a.

Théorème 6. Soient $a_0, \dots, a_n$ des réels distincts, et $b_0, \dots, b_n$ d'auters réels (pas nécessairement distincts). Alors il existe un unique polynôme L de degré au plus n tel que $\forall k \in \{0, \dots, n\}$, $P(a_i) = b_i$. Ce polynôme est appelé polynôme interpolateur de Lagrange.

Démonstration. La démonstration de l'existence est très simple, on construit explicitement un polynôme prenant les $n+1$ valeurs demandées. Pour cela, on commence par définir les $n+1$ polynômes de degré n suivants : $L_i = \dfrac{\prod_{j \neq i}(X - a_j)}{\prod_{j \neq i}(a_i - a_j)}$. Le numérateur est simplement le polynôme de degré n unitaire ayant pour racines tous les nombres a_j sauf a_i (l'entier i étant préalablement fixé), et on le divise ensuite par une constante (non nulle puisque les a_j sont par définition différents de a_i). Par construction, $L_i(a_j) = 0$ si $j \neq i$ pusique a_j est une racine du numérateur. Par ailleurs, $L_i(a_i) = 1$ puisqu'en remplaçant X par a_i, le numérateur est clairement égal au dénominateur. il suffit maintenant de poser $L = \sum_{i=0}^{n} b_i L_i$ pour obtenir un polynôme qui vaut b_i en a_i (dans le calcul de $L(a_i)$, tous les termes de la somme sont nuls sauf celui d'indice i qui vaut $b_i \times 1$). Ce polynôme est de degré au plus n puisqu'il est une somme de polynômes de degré n, il répond donc au problème posé.

Reste à prouver l'unicité : supposons donc que deux polynômes L et Z conviennent. Puisque ces deux polynômes prennant la même valeur en $n+1$ réels distincts, leur différence $L - Z$ admet donc (au moins) $n+1$ racines. Or, $L - Z$ est par hypothèse une différence de deux polynômes dont le degré ne dépasse pas n, donc lui-même de degré inférieur ou égal à n. Il est alors nécessairement nul, ce qui prouve que $Z = L$. □

Exemple : On souhaite déterminer un polynôme de degré 2 vérifiant $P(1) = 3$, $P(2) = 2$ et $P(3) = -1$. On va numéroter les valeurs 1, 2 et 3 plutôt que 0, 1 et 2 pour ne pas créer de confusion inutile, et on définit donc $L_1 = \dfrac{(X-2)(X-3)}{(1-2)(1-3)} = \dfrac{1}{2}X^2 - \dfrac{5}{2}X + 3$; $L_2 = \dfrac{(X-1)(X-3)}{(2-1)(2-3)} = -X^2 + 4X - 3$ et $L_3 = \dfrac{(X-1)(X-2)}{(3-1)(3-2)} = \dfrac{1}{2}X^2 - \dfrac{3}{2}X + 1$ (notez au passage que ces polynômes ne dépendent pas du tout du choix des valeurs b_i). On calcule ensuite $P = 3L_1 + 2L_2 - L_3 = -X^2 + 2X + 2$. On vérifie aisément que le polynôme est bien solution du problème. Bien entendu, les plus courageux peuvent résoudre ce genre de problème en résovant un système de $n+1$ équations à $n+1$ inconnues en recherchant les coefficients du polynôme à partir des conditions sur les valeurs prises.

Théorème 7. Formule de Taylor pour les polynômes.
Soit $P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$, alors $P(X) = \sum_{k=0}^{n} \dfrac{P^(k)(a)}{k!}(X-a)^k$.

Démonstration. Commençons par prouver la formule dans le cas particulier où $P(X) = P_i(X) = X^i$. Dans ce cas, les dérivées du polynôme sont données par $P'(X) = iX^{i-1}$, $P''(X) = i(i-1)X^{i-2}$, …, $P^{(k)}(X) = i(i-1)\dots(i-k+1)X^{i-k} = \dfrac{i!}{(i-k)!}X^{i-k}$ (une récurrence est nécessaire pour prouver ce résultat tout à fait rigoureusement, on s'en passera). On en déduit que $P^{(k)}(a) = \dfrac{i!}{(i-k)!}a^{i-k}$, puis que $\sum_{k=0}^{n} \dfrac{P^(k)(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \dfrac{i!}{(i-k)!k!}a^{i-k}(X-a)^k = \sum_{k=0}^{n} \binom{i}{k}(X-a)^k a^{i-k} = (X-a+a)^i = X^i$ en reconnaissant la formule du binôme de Newton. Certains termes de la somme ne sont pas définis (quand $k > i$), ce qui ne pose pas de problème en considérant qu'ils sont nuls par convention. Pour

prouver la formule pour un polynôme quelconque, on procède ensuite par linéarité : $P = \sum_{i=0}^{n} a_i P_i$ (où les a_i sont les coefficients de P), donc $P(X) = \sum_{i=0}^{n} a_i P_i(X) = \sum_{i=0}^{n} a_i \sum_{k=0}^{n} \frac{P_i^(k)(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{1}{k!}(X-a)^k \sum_{i=0}^{n} a_i P_i^{(k)}(a) = \sum_{k=0}^{n} \frac{1}{k!}(X-a)^k P^{(k)}(a)$ par linéarité des dérivées k-èmes. □

Exemple : Soit $P = 2X^3 - 3X^2 + X - 4$, et posons $a = 2$. On calcule sans difficulté $P(2) = 16 - 12 + 2 - 4 = 2$; $P' = 6X^2 - 6X + 1$ donc $P'(2) = 24 - 12 + 1 = 13$; $P''(2) = 12X - 6$ donc $P''(2) = 18$ et enfin $P'''(2) = 12$. La formule de Taylor affirme alors que $P = 2 + 13(X-2) + 9(X-2)^2 + 2(X-2)^3$. Vous pouvez naturellement tout développer pour vérifier que ça marche. On remarquera que, présentés dans cet ordre, les différents termes de la formule de Taylor sont de plus en plus petits quand on se rapproche de 2.