Chapitre 14 : Polynômes

MPSI Lycée Camille Jullian

28 février 2023

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.

Avant de s'attaquer vraiment à l'algèbre linéaire, ce chapitre servira entre autres 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 chapitre sera également l'occasion d'exploiter les théorèmes vus en arithmétique pour les « copier » dans le cadre des anneaux de polynômes, mais aussi 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. Bref, les polynômes forment un objet d'études central en mathématiques, à la frontière de domaines très variés : algèbre, arithmétique, analyse. C'est pourquoi les applications des méthodes vues dans ce chapitre sont aussi nombreuses et variées.

Objectifs du chapitre :

- savoir factoriser ou effectuer une division euclidienne sur des polynômes à coefficients réels ou complexes.
- maîtriser la factorisation d'un polynôme en produits de facteurs irréductibles, dans $\mathbb{R}[X]$ comme dans $\mathbb{C}[X]$.
- comprendre ce que signifie la formule de Taylor d'un point de vue analytique.

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

Dans toute cette partie, comme précédemment dans le chapitre de calcul matriciel, la notation $\mathbb{K}$ désigne un corps quelconque qui sera en pratique la plupart du temps $\mathbb{R}$ ou $\mathbb{C}$, avec quelques rares incursions dans le corps $\mathbb{Q}$ des rationnels.

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 l'**indéterminée** destinée à être remplacée par n'importe quel objet pour lequel le calcul de P peut avoir un sens (des nombres réels ou complexes feront bien sûr l'affaire, mais aussi tout objet mathématique pour lequel on peut calculer des puissances et qu'on peut multiplier par des éléments de $\mathbb{K}$, notamment les matrices carrées, les suites ou les fonctions).

Remarque 1. Il est important de ne pas identifier (surtout si $\mathbb{K} = \mathbb{R}$) le polynôme avec la fonction polynômiale associée. C'est en partie pour cela que l'indéterminée est notée X et non x quand on parle de polynômes formels : X n'est pas forcément un nombre. Ainsi, si $P = X^2 + 3X + 1$, on peut calculer, pour une matrice $M \in \mathcal{M}_3(\mathbb{R})$, $P(M) = M^2 + 3M + I_3$ (attention à ne pas oublier de remplacer le 1, qu'on devrait techniquement noter X^0, par l'élément neutre de l'ensemble où se trouve l'objet auquel on applique le polynôme). On peut même calculer, pour une fonction comme ln, $P(\ln)$ qui sera la fonction $f : x \mapsto \ln^2(x) + 3\ln(x) + 1$.

Définition 2. Soit $P = \sum_{k=0}^{k=n} a_k X^k$ un polynôme, avec $a_n \neq 0$.

- Les nombres a_k sont les **coefficients** du polynôme P
- l'entier n est le **degré** de P (souvent noté $d^\circ(P)$)
- le coefficient a_n est le **coefficient dominant** de P
- un polynôme est **unitaire** si ce coefficient dominant est égal à 1
- un **monôme** est un polynôme n'ayant qu'un seul coefficient non nul (tout polynôme est donc par définition une somme de monômes).

Remarque 2. Par convention, le polynôme nul a pour degré $-\infty$. C'est relativement cohérent avec les propriétés énoncées ci-dessous.

Définition 3. On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$, sans distinction de degré. On note aussi, pour tout entier naturel n, $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n à coefficients dans $\mathbb{K}$.

Remarque 3. On considère l'ensemble des polynômes vérifiant la condition $d^\circ(P) \leqslant n$ et non pas $d^\circ(P) = n$ car ce dernier ensemble ne serait pas stable par somme, comme on va le voir ci-dessous, et ne serait pour cette raison pas muni d'une structure d'espace vectoriel.

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

Proposition 1. La somme de polynômes est associative, commutative, et admet pour élément neutre le polynôme nul (noté 0) dont tous les coefficients sont nuls. De plus, 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 donc $P + (-P) = 0$. Autrement dit, $(\mathbb{K}[X], +)$ est un groupe commutatif.

Démonstration. Tout est absolument trivial. □

Définition 5. Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{p} b_k X^k$ deux polynômes appartenant à $\mathbb{K}[X]$, 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. L'élément neutre pour le produit de polynômes est le polynôme constant 1. L'ensemble $(\mathbb{K}[X], +, \times)$ est un anneau commutatif intègre.

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 (ce qui a bien un sens, cela revient à parcourir cette somme « à l'envers »). 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. Enfin, l'intégrité de l'anneau découle du fait que, par définition même du produit, on aura $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$ pour deux polynômes non nuls P et Q, leur produit ne peut donc pas être nul (il est de degré positif). □

Remarque 4. On peut aussi munir l'ensemble $\mathbb{K}[X]$ d'un produit extérieur par les éléments de $\mathbb{K}$ en identifiant simplement ces deniers avec les polynômes constants (ce qu'on fait de fait en permanence), ce qui munit alors $\mathbb{K}[X]$ d'une structure d'espace vectoriel sur $\mathbb{K}$. Vous aurez bien sûr droit à une définition complète (et affreuse) dans un chapitre ultérieur, mais l'idée est là : un produit par des constantes et une addition qui vérifient quelques propriétés élémentaires naturelles. C'est d'ailleurs pour que $\mathbb{K}_n[X]$ soit un sous-espace vectoriel de $\mathbb{K}[X]$ qu'on a inclus dans cet ensemble tous les polynômes de degré strictement inférieur à n (pour être un sous-espace vectoriel, un sous-ensemble doit notamment être un sous-groupe, donc stable par somme, ce qui ne serait pas le cas de l'ensemble des polynômes de degré exactement égal à n).

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 (on l'a d'ailleurs déjà indiqué plus haut pour le produit). L'inégalité 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 5. Les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants (non nuls).

Définition 6. 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 Racines d'un polynôme.

2.1 Division euclidienne.

Définition 7. Le polynôme P est **divisible** par Q (ou Q divise P, ou encore P est un multiple de Q) si le reste de la division euclidienne de P par Q est nul. Autrement dit, il existe un troisième polynôme R tel que $P = QR$. On peut le noter, comme pour les entiers, $Q \mid P$.

Remarque 6. La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{K}[X]$: elle est transitive et réflexive mais pas antisymétrique. Plus précisément, deux polynômes P et Q sont divisibles l'un par l'autre « dans les deux sens » s'il existe une constante $\lambda \in \mathbb{K}$ telle que $P = \lambda Q$. On parle alors de polynômes **associés**. Les propriétés de la relation de divisibilité dans $\mathbb{K}[X]$ sont extrêmement similaires à celles déjà vues sur $\mathbb{Z}$ (ce qui explique la similarité des théorèmes arithmétiques énoncés plus loin dans ce chapitre). Par exemple, si R divise les deux polynômes P et Q, alors R divise toute combinaison linéaire de P et Q. Si P divise Q, alors P^k divise Q^k pour tout entier naturel k.

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

- $A = BQ + R$
- $d^\circ(R) < d^\circ(B)$

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'existence 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 $a_n X^{n+1}$ son terme dominant, et $b_p X^p$ 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, les termes de différents degrés jouant le rôle joué par les différents chiffres de l'écriture décimale dans une division entière, par exemple pour diviser $X^4-3X^3+5X^2+X-3$ par X^2-2X+1 :

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

Conclusion : $X^4-3X^3+5X^2+X-3=(X^2-X+2)(X^2-2X+1)+6X-5$. Rappelons que 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. Il est par contre hors de question dans le cas d'une division de polynômes de pousser les calculs « après la virgule » comme on peut le faire pour une division entière.

Exemple : La division euclidienne peut être utilisée comme alternative aux suites récurrentes pour calculer les puissances d'une matrice dont on connait un polynôme annulateur. Prenons par exemple la matrice $A=\begin{pmatrix}2&2&1\\1&3&1\\1&2&2\end{pmatrix}$. On calcule $A^2=\begin{pmatrix}7&12&6\\6&13&6\\6&12&7\end{pmatrix}$, puis on constate que $A^2=6A-5I_3$. On peut alors dire que $P=X^2-6X+5$ est un polynôme annulateur de la matrice A. On peut déduire plusieurs choses à partir de ce polynôme annulateur :

- la matrice est inversible dès lors que le polynôme annulateur a un coefficient constant non nul (méthode déjà vue, on isole I_3 dans l'égalité puis on factorise l'autre membre par A. Ici, on obtiendrait $-\frac{1}{5}A^2+\frac{6}{5}A=I_3$, donc A est inversible et $A^{-1}=-\frac{1}{5}A+\frac{6}{5}I_3$.
- on peut calculer A^n pour tout entier naturel n en utilisant la méthode des suites récurrentes ou le calcul plus rapide suivant : le polynôme annulateur X^2-6X+5 se factorise sous la forme $(X-1)(X+5)$ (1 en est une racine évidente). La division euclidienne du monôme X^n par X^2-6X+5 peut s'écrire sous la forme $X^n=Q(X^2-6X+5)+a_nX+b_n$ (le reste étant de degré strictement plus petit que celui de P, il est ici de degré inférieur ou égal à 1). On peut calculer rapidement a_n et b_n en évaluant cette égalité pour les deux racines de P : pour $X=1$, on aura $P(1)=0$, donc $1=a_n+b_n$. De même pour $X=5$ on aura $5^n=5a_n+b_n$. En soustrayant ces deux équations on trouve $4a_n=5^n-1$, soit $a_n=\dfrac{5^n-1}{4}$. On en déduit que $b_n=1-a_n=\dfrac{5-5^n}{4}$. Il ne reste plus qu'à évaluer la division euclidienne pour $X=A$ (on a bien entendu le droit !) pour que le miracle s'opère : $A^n=Q(A)P(A)+a_nA+b_nI_3$, donc $A^n=a_nA+b_nI_3$ (puisque $P(A)=0$). Les suites (a_n) et (b_n) ne sont en fait rien d'autre que celles qu'on aurait obtenues par la méthode « classique » mais, en maîtrisant bien la division euclidienne, on les calcule plus rapidement.

2.2 Racines et factorisation.

Définition 8. Soit $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$. On dit que a est une **racine** du polynôme P si $P(a)=0$.

Remarque 7. On identifie ici le polynôme et la fonction polynômiale associée pour le calcul de $P(a)$, comme ce sera le cas dans tout 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. Les nombres complexes vérifiant $P(a)=0$ seront

bien qualifiés de racines, on précisera les choses si besoin dans les énoncés en parlant des racines réelles ou des racines complexes du polynôme. Par contre, une matrice vérifiant une relation du type $A^2-3A=0$ ne sera pas considérée comme une racine du polynôme $P=X^2-3X$, on dira simplement que le polynôme P **annule** la matrice A.

Proposition 5. Le nombre a est racine du polynôme P si et seulement si P est divisible par $X-a$.

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, $\exists k \in \mathbb{K}$, $P=Q(X-a)+k$. 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 $a=2$, donc $a=2$, $b-a=-3$ donc $b=-1$, et $c-b=5$ donc $c=4$ (ce qui est cohérent avec la dernière condition), 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 $a_1, a_2, \ldots, a_k$ comme racines distinctes si et seulement si il est divisible par $\prod_{i=1}^{k}(X-a_i)$.

Démonstration. On peut procéder par récurrence (forte) 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 $E \subset \mathbb{K}$ est un ensemble infini tel que, $\forall x \in E$, $P(x) = Q(x)$, alors les polynômes P et Q sont égaux.

Démonstration. Dans ce cas, $P - Q$ est un polynôme admettant un ensemble infini de racines, donc $P - Q = 0$ d'après le corollaire précédent. C'est bien ce principe qu'on utilise pour identifier les coefficients de deux polynômes correspondant à des expressions polynômiales égales. □

2.3 Multiplicité d'une racine.

Définition 9. Soit P un polynôme et a une racine de P. On dit que a est une racine **de multiplicité** $k \in \mathbb{N}^*$ si P est divisible par $(X-a)^k$, mais pas par $(X-a)^{k+1}$.

Remarque 8. Cela revient en gros à dire que la racine « compte pour k racines » lors de la factorisation du polynôme. En particulier, on peut facilement affiner un des corollaires du paragraphe précédent de la façon suivante : un polynôme P de degré n admet au maximum n racines comptées avec multiplicité. Ainsi, un polynôme de degré 5 admettant une racine triple (c'est-à-dire d'ordre de multiplicité 3), ne peut avoir (au maximum) que deux autres racines, car la factorisation de P par $(X-a)^3$ laissera un deuxième facteur de degré 2.

Définition 10. 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 9. 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 usuelles, en particulier la formule de Leibniz : $PQ^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$. Cette formule, que nous reverrons dans le prochain chapitre consacré à la dérivation, se démontre exactement via la même réurrence que la formule du binôme de Newton avec laquelle la similarité formelle est frappante.

Proposition 6. Une racine a est 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. □

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 $P(2) = 16 - 2\times 8 - 19\times 4 + 68\times 2 - 60 = 16 - 16 - 76 + 136 - 60 = 0$ et $P' = 4X^3 - 6X^2 - 38X + 68$, 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 :

$$\begin{array}{rcccccccc|l}
X^4 & - & 2X^3 & - & 19X^2 & + & 68X & - & 60 & X^2 - 4X + 4 \\
\cline{10-10}
- \ (X^4 & - & 4X^3 & + & 4X^2) & & & & & X^2 + 2X - 15 \\
 & & 2X^3 & - & 23X^2 & + & 68X & - & 60 & \\
 & - & (2X^3 & - & 8X^2 & + & 8X) & & & \\
 & & & - & 15X^2 & + & 60X & - & 60 & \\
 & & & - & (-15X^2 & + & 60X & - & 60) & \\
 & & & & & & & & 0 &
\end{array}$$

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.

Définition 11. Un polynôme P est **scindé** s'il peut s'écrire comme produit de polynômes de degré 1 (autrement dit s'il a un nombre de racines, comptées avec multiplicité, 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 $\mathbb{C}[X]$ est scindé.

Démonstration. Ce résultat fondamental a déjà été croisé dans le chapitre sur les nombres complexes sous une forme légèrement différente. Nous n'avons toujours pas les moyens de le démontrer maintenant, mais il suffit pour le prouver de montrer qu'un polynôme de degré au moins 1 appartenant à $\mathbb{C}[X]$ admet toujours une racine (on applique ensuite ce résultat récursivement après avoir commencé à factoriser le polynôme, jusqu'à retomber sur des facteurs qui sont tous de degré 1). □

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

2.4 Relations coefficients-racines.

Proposition 7. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, et α_1, α_2, ..., α_n ses racines (éventuellement répétées plusieurs fois en cas de racines multiples). On a alors les relations suivantes entre les coefficients et les racines de P :

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

Démonstration. Il suffit d'identifier la forme développée du polynôme et sa forme factorisée pour obtenir ces relations. On part de la forme factorisée $P = a_n(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_n)$ (on connait toutes les racines), et on développe brutalement ce produit, le terme dominant sera alors $a_n X^n$ (ce qui ne donne évidemment aucune information), le terme de degré $n-1$ est obtenu en additionnant n termes provenant du produit d'une des racines (avec un petit signe $-$) par $n-1$ facteurs X piochés dans les autres parenthèses, il vaut donc $a_n(-\alpha_1 X^{n-1} - \alpha_2 X^{n-1} - \cdots - \alpha_n X^{n-1})$, qu'on identifie à $a_{n-1}X^{n-1}$ pour obtenir la première formule annoncée. Les autres sont obtenues de la même façon, on ne détaillera pas rigoureusement cette démonstration hors-programme. La dernière relation correspond au terme constant, obtenu en multipliant les opposés des racines présentes dans chaque parenthèse, donc égal à $a_n \times (-1)^n \prod_{k=1}^{n} \alpha_i$. □

Définition 12. En notant $\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}$, la k-ème relation coefficient-racines s'écrit simplement $\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$. Les nombres σ_k sont appelés **fonctions symétriques** des racines du polynôme.

Exemple : Pour un polynôme de degré 4 ayant pour racines a, b, c et d, les formules deviennent :

- $a + b + c + d = -\frac{a_3}{a_4}$
- $ab + ac + ad + bc + bd + cd = \frac{a_2}{a_4}$
- $abc + abd + acd + bcd = -\frac{a_1}{a_4}$
- $abcd = \frac{a_0}{a_4}$

Exemple : On cherche à factoriser le polynôme $4X^3 - 4X^2 - 15X + 18$, sachant qu'un ami nous a glissé un indice : deux de ses racines ont une somme égale à 3.

On utilise les relations coefficients-racines. En notant a et b les racines dont la somme est égale à 3

et c la troisième racine de P, on aura le système $\begin{cases} 3+c & = & 1 \\ ab+ac+bc & = & -\dfrac{15}{4} \\ abc & = & -\dfrac{9}{2} \end{cases}$. La première équation nous donne immédiatement $c=-2$, on peut alors remplacer dans la dernière équation pour trouver $ab=\dfrac{9}{4}$. On connait la somme et le produit des deux racines restantes, qui sont donc solutions de l'équation $x^2-3x+\dfrac{9}{4}=0$. Cette équation a pour discriminant $\Delta=9-9=0$ et admet donc pour racine double $x=\dfrac{3}{2}$. On en déduit la factorisation souhaitée, en n'oubliant pas le coefficient dominant : $P=4\left(X-\dfrac{3}{2}\right)^2(X+2)$.

Variation sur le même thème : on reprend le même polynôme, mais cette fois, l'indice qui nous a été glissé est la présence d'une racine double.

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, $\left(\dfrac{3}{2}\right)^2\times\alpha=\dfrac{9}{4}\alpha$, on en déduit que $\alpha=-2$, et $P=4\left(X-\dfrac{3}{2}\right)^2(X+2)$.

3 Arithmétique dans $\mathbb{K}[X]$.

3.1 Polynômes irréductibles.

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.

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

Remarque 11. Attention, la notion de polynôme irréductible dépend fortement du corps de base choisi. Ainsi, le polynôme X^2+4 est irréductible dans $\mathbb{R}[X]$ (si on pouvait le factoriser, ce serait comme produit de deux polynômes de degré 1, ce qui supposerait qu'il ait deux racines réelles. Or ce n'est pas le cas). Par contre, il n'est pas du tout irréductible dans $\mathbb{C}[X]$ puisqu'on peut l'écrire sous la forme $(X+2i)(X-2i)$.

Théorème 3. 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.

Démonstration. Le premier énoncé est une conséquence directe du théorème de d'Alembert-Gauss : tout polynôme de degré supérieur ou égal à 2 dans $\mathbb{C}[X]$ admet une racine et ne peut donc pas être irréductible. Pour le cas des coefficients réels, cela découlera de la démonstration du théorème de décomposition énoncé plus bas. □

3.2 PGCD et PPCM dans $\mathbb{K}[X]$.

Définition 14. Si P et Q sont deux polynômes non nuls, on appelle PGCD de P et Q tout polynôme de degré maximal divisant simultanément P et Q. De même, on appelle PPCM de P et Q tout polynôme de degré minimal qui est à la fois multiple de P et de Q.

Remarque 12. Tous les PGCD de deux polynômes P et Q sont associés. On appellera donc « **le** PGCD de P et Q » l'unique PGCD unitaire de P et Q. On le notera usuellement $P \wedge Q$. On notera de même $P \vee Q$ **le** PPCM de P et Q, c'est-à-dire l'unique PPCM unitaire des deux polynômes.

Théorème 4. Algorithme d'Euclide du calcul de $P \wedge Q$.

Comme dans le cas des entiers naturels, on peut calculer $P \wedge Q$ à l'aide de la procédure algorithmique suivante : on pose $R_0 = P$, $R_1 = Q$ puis, pour tout $n \geqslant 2$, R_n est le reste de la division euclidienne de R_{n-2} par R_{n-1}. On obtiendra toujours $R_n = 0$ après un nombre fini d'étapes, et R_{n-1} sera alors égal à $P \wedge Q$.

On peut même, exactement comme pour les entiers, calculer les coefficients d'une relation de Bézout reliant les polynômes P et Q (cf plus bas) via l'algorithme d'Euclide étendu, en posant $U_0 = 1$, $U_1 = 0$, $R_0 = 0$, $R_1 = 1$ et en leur appliquant les relations de récurrence $U_{n+1} = U_{n-1} - Q_n U_n$ et $V_{n+1} = V_{n-1} - Q_n V_n$. Par exemple, si on pose $P = 6X^4+8X^3-7X^2-5X-2$ et $Q = 6X^3-4X^2-X-1$:

- on effectue la division de P par Q, et on obtient $6X^4+8X^3-7X^2-5X-2 = (X+2)(6X^3-4X^2-X-1)+2X^2-2X$. On pose donc $Q_2 = X+2$, $R_2 = 2X^2-2X$, et $U_2 = 1$, $V_2 = -X-2$.
- on effectue la division euclidienne de Q par R_2, qui donne $6X^3 - 4X^2 - X - 1 = (3X + 1)(2X^2 - 2X) + X - 1$. On pose donc $Q_3 = 3X + 1$, $R_3 = X - 1$, et $U_3 = -3X - 1$, $V_3 = 1 + (X + 2)(3X + 1) = 3x^2 + 7X + 3$.
- on constate que $R_2 = 2XR_3$, le reste de la prochaine division euclidienne sera nul. On conclut que $P \wedge Q = X - 1$, et que $(3X^2 + 7X + 3)Q - (3X + 1)P = X - 1$.

Définition 15. Comme pour les entiers, on étend la définition du PGCD et du PPCM à toute famille finie de polynômes.

Définition 16. Deux polynômes P et Q sont **premiers entre eux** si $P \wedge Q = 1$.

Les polynômes $P_1, P_2, \ldots, P_k$ sont **premiers entre eux dans leur ensemble** si $PGCD(A_1, A_2, \ldots, A_k) = 1$.

Remarque 13. Comme dans le cas des entiers, des polynômes premiers entre eux dans leur ensemble ne sont pas forcément premiers entre eux deux à deux.

Théorème 5. Théorème de Bézout.
Deux polynômes P et Q sont premiers entre eux si et seulement s'il existe un couple de polynômes (A, B) tels que $AP + BQ = 1$. Plus généralement, il existe toujours un couple de polynômes tels que $AP + BQ = P \wedge Q$.

Théorème 6. Théorème de Gauss.
Si P et Q sont deux polynômes premiers entre eux, et $P \mid QR$, alors $P \mid R$.

3.3 Décomposition en produit de polynômes irréductibles.

Théorème 7. Tout polynôme unitaire $P \in \mathbb{R}[X]$ peut se factoriser sous la forme $P = \prod_{i=1}^{p}(X-a_i)^{\alpha_i} \prod_{j=1}^{q}(X^2+b_jX+c_j)^{\beta_j}$. Dans cette écriture :

- $a_1, a_2, \ldots, a_n$ sont les racines réelles du polynôme P
- α_i représente la multiplicité de la racine a_i
- les polynômes du second degré $X^2+b_jX+c_j$ sont des polynômes à discriminant strictement négatif
- β_j représente la multiplicité des racines (complexes) du polynôme $X^2+b_jX+c_j$

Cette décomposition est unique à l'ordre des facteurs près.

Exemple : On souhaite factoriser le plus possible le polynôme $P = X^6 - 1$. Que le calcul s'effectue dans $\mathbb{R}[X]$ ou dans $\mathbb{C}[X]$, il faut de toute façon commencer par trouver toutes les racines complexes du polynôme. C'est ici immédiat puisqu'il s'agit des racines sixièmes de l'unité complexe, donc $z_1 = 1$, $z_2 = e^{i\frac{\pi}{3}}$, $z_3 = e^{i\frac{2\pi}{3}}$, $z_4 = -1$, $z_5 = e^{i\frac{4\pi}{3}}$ et $z_6 = e^{i\frac{5\pi}{3}}$. La décomposition de P dans $\mathbb{C}[X]$ en découle immédiatement, en écrivant ces racines sous forme algébrique (et en plaçant les racines réelles en premier, ce qui n'est pas du tout une obligation) : $P = (X-1)(X+1)\left(X-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)\left(X-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$.

Pour passer dans $\mathbb{R}[X]$, il faut réussir à regrouper certains facteurs à coefficients complexes et à effectuer leur produit de façon à ce que le résultat ait des coefficients réels. Le théorème énoncé ci-dessus stipule qu'on peut toujours y arriver à l'aide de produits de deux polynômes (pas de facteurs de dégré plus grand que 2 à la fin), ce qui est en pratique très simple en regroupant les facteurs dont les racines sont conjuguées. Ici, par exemple, $(X-e^{\frac{i\pi}{3}})(X-e^{i\frac{5\pi}{3}}) = X^2-X+1$. On obtient la décomposition suivante pour P dans $\mathbb{R}[X]$: $P = (X-1)(X+1)(X^2-X+1)(X^2+X+1)$.

Démonstration. Généralisons simplement les constatations faites sur l'exemple que nous venons de développer. Si on trouve parmi les racines complexes d'un polynôme P une racine a et son conjugué $\overline{a}$, alors $(X-a)(X-\overline{a}) = X^2-(a+\overline{a})X+a\overline{a} = X^2-2\text{Re}\,(a)X+|a|^2$ est bien un polynôme de degré 2 à coefficients réels (et à discriminant nécessairement négatif puisque ses racines sont complexes). Or, lorsque a est racine complexe d'un polynôme à coefficients réels, $\overline{a}$ l'est aussi : $P(\overline{a}) = \sum_{k=1}^{n} a_k\overline{a}^k = \sum_{k=1}^{n}\overline{a_k a^k} = \overline{P(a)} = 0$. De plus, la multiplicité de a sera toujours la même que celle de $\overline{a}$ puisque le raisonnement précédent peut s'appliquer à l'identique aux polynômes dérivés successifs de P (qui garderont évidemment des coefficient réels). On peut donc toujours effectuer la procédure détaillée dans l'exemple (factorisation dans $\mathbb{C}[X]$, regroupement des facteurs correspondant à des racines conjuguées) pour obtenir la forme annoncée dans l'énoncé du théorème. □

Théorème 8. Tout polynôme $P \in \mathbb{K}[X]$ peut s'écrire comme produit de facteurs irréductibles.

Démonstration. Ce dernier théorème n'est qu'une façon légèrement différente d'énoncer la factorisation des polynômes vue un peu plus haut. □

Remarque 14. Ces théorèmes de factorisation sont l'équivalent dans $\mathbb{K}[X]$ du théorème de décomposition en produit de facteurs premiers dans $\mathbb{N}$. Les polynômes irréductibles jouent le même rôle que les facteurs premiers (éléments impossibles à décomposer sous forme de produit), et toute la démonstration découle de façon naturelle de l'existence d'un théorème de division euclienne dans les deux ensembles.

4 Compléments.

Les deux compléments présentés dans cette dernière partie, qui sont totalement indépendants l'un de l'autre, reposent toutefois sur un même principe, qui est fortement lié à la notion d'espace vectoriel que nous ne tarderons pas à étudier : pour décrire un polynôme de degré n, on a besoin de $n+1$ informations indépendantes (cette valeur $n+1$ correspond techniquement à la dimension de l'espace vectoriel $\mathbb{K}_n[X]$). La façon la plus simple de le faire est de donner les $n+1$ coefficients du polynôme, mais cette information n'est par exemple pas immédiatement exploitable pour obtenir des informations sur la représentation graphique de la fonction polynômiale correspondante (pour un polynôme à coefficients réels). Savoir par exemple qu'un polynôme de degré 5 a un coefficient de degré 3 égal à 1 ne donne aucune information concrète (point de la courbe, tangente, etc). Nous allons étudier deux autres façons de décrire un polynôme à l'aide de $n+1$ informations, qui sont nettement plus directement exploitables graphiquement :

- 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 (on connait $n+1$ points de la courbe).
- la dernière méthode que nous verrons concentre au contraire 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.

4.1 Polynômes interpolateurs de Lagrange.

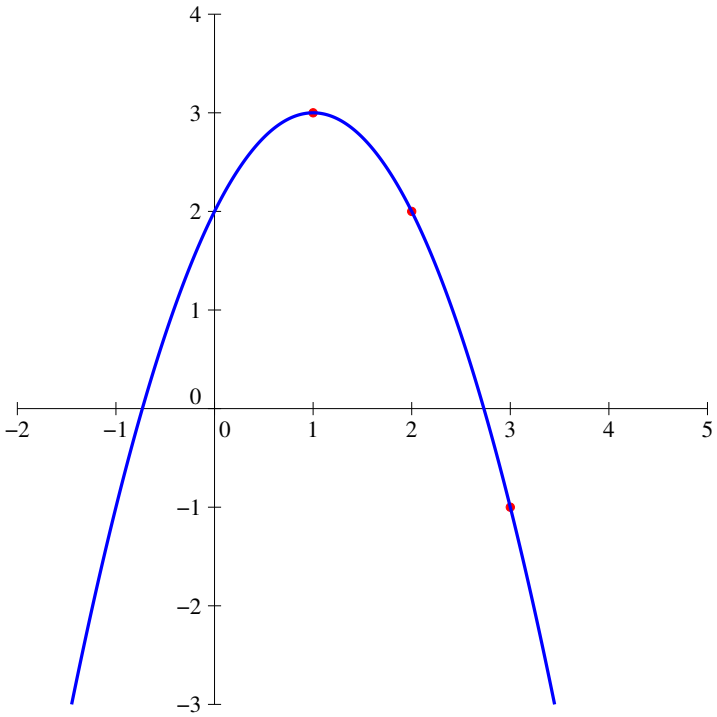
Théorème 9. Soit $(a_0, \ldots, a_n)$ une liste de réels deux à deux distincts, et $(b_0, \ldots, b_n)$ une deuxième liste de réels (pas nécessairement distincts). Alors il existe un unique polynôme $P \in \mathbb{R}_n[X]$ de degré au plus n tel que $\forall k \in \{0, \ldots, n\}$, $P(a_i) = b_i$. Ce polynôme est appelé polynôme interpolateur de Lagrange.

Démonstration. La démonstration de l'existence est très simple puisqu'on construit explicitement le polynôme prenant les $n+1$ valeurs demandées. Pour cela, on commence par définir $n+1$ polynômes de degré n suivants (ce sont techniquement eux qu'on appelle polynômes de Lagrange) : $L_i = \dfrac{\prod_{j \neq i}(X - a_j)}{\prod_{j \neq i}(a_i - a_j)}$. 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) de façon à avoir $L_i(a_i) = 1$. Par construction, on a par ailleurs $L_i(a_j) = 0$ si $j \neq i$ puisque a_j est une racine du numérateur. Le polynôme L_i est donc une solution du problème d'interpolation particulier où une des valeurs imposées est égale à 1 et toutes les autres à 0. Il suffit maintenant de poser $P = \sum_{i=0}^{n} b_i L_i$ pour obtenir un polynôme qui prend comme valeur 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 P et Q conviennent. Puisque ces deux polynômes prennant la même valeur en $n+1$ réels distincts, leur différence $P-Q$ admet donc (au moins) $n+1$ racines. Or, $P-Q$ 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 $P = Q$. □

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.



Remarque 15. Plus généralement, tous les polynômes vérifiant $P(a_i) = b_i$ (sans imposer un degré égal à n) sont de la forme $P_0 + Q\prod_{i=0}^{n}(X - a_i)$, où P_0 est l'unique solution de degré au plus n décrite ci-dessus. C'est même assez évident : un tel polynôme convient (le produit de droite s'annule pour

tous les a_i donc ne changera pas la valeur du polynôme en a_i), et si P est un polynôme solution, alors $P - P_0$ admet tous les nombres a_i comme racines, donc se factorise par $\prod_{i=0}^{n}(X - a_i)$, ce qui correspond exactement à la forme donnée.

4.2 Formule de Taylor.

Le principe de la formule de Taylor, que nous reverrons sous d'autres formes très bientôt puisqu'elle est à la base des développements limités qui constitueront le coeur du principal chapitre d'analyse du second semestre, est de généraliser la notion de tangente à une courbe à des polynômes de degré plus grand que 1. On cherche par exemple, pour une fonction donnée, la parabole (courbe d'un polynôme de degré 2) qui « colle » le plus possible à la courbe au voisinage d'un point donné. La formule de Taylor donne directement l'équation de cette parabole (et des courbes de degré supérieur analogues) à partir des valeurs prises par les dérivées d'ordre supérieur de la fonction. Bien sûr, si on applique la formule à un polynôme, on est dans un cas particulier puisque la courbe polynômiale la plus proche de celle de la fonction sera évidemment celle du polynôme lui-même. La formule est malgré tout intéressante parce qu'elle donne des coefficients qu'on retrouvera dans toutes les versions de la formule de Taylor, et aussi parce qu'elle montre qu'on peut reconstituer intégralement un polynôme de degré n à partir des valeurs de ses dérivées en un même point a.

Théorème 10. Formule de Taylor, version polynômes.
Soit $P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$, alors $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

Démonstration. On va se contenter de prouver la formule dans le cas particulier où $P(X) = X^n$. Dans ce cas, les dérivées du polynôme sont données par $P'(X) = nX^{n-1}$, $P''(X) = n(n-1)X^{n-2}$, ..., $P^{(k)}(X) = n(n-1)\dots(n-k+1)X^{n-k} = \frac{n!}{(n-k)!}X^{n-k}$ (une récurrence est nécessaire pour prouver ce résultat tout à fait rigoureusement, on s'en passera). On en déduit que $P^{(k)}(a) = \frac{n!}{(n-k)!}a^{n-k}$, puis que $\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{n!}{(n-k)!k!}a^{n-k}(X-a)^k = \sum_{k=0}^{n} \binom{n}{k}(X-a)^k a^{n-k} = (X-a+a)^n = X^n$ en reconnaissant la formule du binôme de Newton. □

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, ou si on on préfère que les formules obtenues en ne prenant qu'une partie des termes du membre de droite deviennent des approximations de plus en plus précises de $P(X)$.