POLYNÔMES

Dans tout ce chapitre, $\mathbb{K}$ est l'un des corps $\mathbb{R}$ ou $\mathbb{C}$. La plupart des résultats présentés demeurent vrais pour un corps $\mathbb{K}$ quelconque — $\mathbb{Q}$ par exemple — mais nous ne nous en préoccuperons pas.

1 CONSTRUCTION DES POLYNÔMES

Jusqu'ici, vous n'avez jamais distingué les polynômes des fonctions polynomiales, qui sont pour vous toutes les fonctions sur $\mathbb{R}$ de la forme $x \longmapsto a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ avec $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{R}$. Nous allons voir dans ce chapitre qu'en fait **NON, LES POLYNÔMES NE SONT PAS DES FONCTIONS.**

Notons par exemple P le polynôme $3X^2 + 4X + 1$. Calculer $P(5)$, c'est transformer 5 en un autre nombre conformément à certaines opérations élémentaires — puissances, multiplication par un réel et addition. Or il y a tout un tas de mondes mathématiques dans lesquels on sait calculer des puissances, multiplier par un réel et additionner les objets :

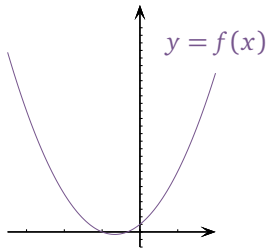
— le corps $\mathbb{R}$ bien sûr, d'où la possibilité de calculer $P(5)$,

— l'anneau $\mathcal{M}_n(\mathbb{R})$, d'où la possibilité de calculer $P(A)$ pour tout $A \in \mathcal{M}_n(\mathbb{R})$,

— l'anneau $\mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, d'où la possibilité de noter $P(\exp)$ la fonction $x \longmapsto 3\mathrm{e}^{2x} + 4\mathrm{e}^x + 1$.

En fait, dans tout anneau A dans lequel on sait multiplier par un réel, on peut poser $P(a) = 3a^2 + 4a + 1_A$ pour tout $a \in A$, mais il faut renoncer pour cela à l'idée qu'un polynôme est une fonction car la fonction $x \longmapsto 3x^2 + 4x + 1$ est définie sur $\mathbb{R}$, pas sur $\mathcal{M}_n(\mathbb{R})$ ou $\mathbb{R}^{\mathbb{R}}$. Finalement, on ne sait toujours pas ce qu'est le polynôme $P = 3X^2 + 4X + 1$, mais ce n'est pas la gentille fonction $x \overset{f}{\longmapsto} 3x^2 + 4x + 1$ en tout cas.

Le piège, c'est que jusqu'ici, quand on vous définissait une fonction polynomiale, on vous donnait aussi ses coefficients. Et quand on connaît la suite $(1, 4, 3)$ des coefficients de f, on peut facilement calculer toutes ses valeurs, par exemple $f(5) = 3 \times 5^2 + 4 \times 5 + 1 = 96$. À l'inverse, quand on connaît f comme fonction, c'est-à-dire par la donnée complète de ses valeurs, il est difficile de remonter jusqu'aux coefficients. Vous pouvez tenter l'expérience sur la figure ci-contre, vous n'y verrez pas les coefficients de f.



Dans ces conditions, il vaut mieux renoncer à faire des polynômes des fonctions et privilégier ce qui compte le plus en eux, à savoir leurs coefficients.

Définition **(Polynôme à une indéterminée à coefficients dans $\mathbb{K}$)** On appelle *polynôme (à une indéterminée) à coefficients dans* $\mathbb{K}$ toute suite *presque nulle* d'éléments de $\mathbb{K}$, i.e. toute suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ dont tous les éléments sont nuls à partir d'un certain rang. Pour tout $k \in \mathbb{N}$, le coefficient a_k est appelé le *coefficient de degré* k du polynôme.

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ si on choisit de noter X l'*indéterminée*.

Conformément à cette définition, un polynôme est une **SUITE** de la forme $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$ à coefficients dans $\mathbb{K}$. Nous pourrons bientôt **NOTER** $a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ une telle suite, mais pas tout de suite. Gardez tout de même cet objectif en tête, il vous aidera à comprendre les prochaines définitions.

Quoi qu'on pense de son abstraction, la définition précédente rend au moins trivial le résultat suivant, si l'on n'oublie pas ce que c'est qu'une suite. Le résultat analogue sur les **FONCTIONS** polynomiales est autrement délicat !

Théorème **(Identification des coefficients)** Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

Définition **(Polynôme constant, polynôme nul)** On appelle *polynôme constant* de $\mathbb{K}[X]$ tout polynôme $(\lambda, 0, 0, \ldots)$ avec $\lambda \in \mathbb{K}$. Un tel polynôme sera simplement noté λ.

Avec cette notation, le polynôme 0 est appelé le *polynôme nul*.

Définition (Degré d'un polynôme, coefficient dominant, polynôme unitaire) Soit $P=(a_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$ un polynôme NON NUL. Le plus grand indice k pour lequel $a_k\neq 0$ est appelé le *degré de P* et noté $\deg(P)$.

Le coefficient de degré $\deg(P)$ de P est appelé son *coefficient dominant*. S'il est égal à 1, on dit que P est *unitaire*.

Par convention, le polynôme nul est de degré $-\infty$: $\deg(0)=-\infty$.

Exemple $7X^4-X^3+2X^2-3X-5$ a pour degré 4 et coefficient dominant 7, tandis que X^3-4X^2+3X+5 est unitaire.

À présent, les polynômes étant des suites : $\mathbb{K}[X]\subset\mathbb{K}^{\mathbb{N}}$. Mais comme $\mathbb{K}$ est un groupe additif, $\mathbb{K}^{\mathbb{N}}$ est un groupe pour la loi d'addition définie par $(u_k)_{k\in\mathbb{N}}+(v_k)_{k\in\mathbb{N}}=(u_k+v_k)_{k\in\mathbb{N}}$ pour tous $(u_k)_{k\in\mathbb{N}},(v_k)_{k\in\mathbb{N}}\in\mathbb{K}^{\mathbb{N}}$. Montrons que $\mathbb{K}[X]$ est un sous-groupe de $\mathbb{K}^{\mathbb{N}}$. Tout d'abord $(0)_{n\in\mathbb{N}}\in\mathbb{K}[X]$. Ensuite, pour tous $P=(a_k)_{k\in\mathbb{N}},Q=(b_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$, nous pouvons nous donner un rang N à partir duquel $a_k=b_k=0$. Alors $a_k-b_k=0$ pour tout $k\geqslant N$, donc $P-Q\in\mathbb{K}[X]$.

Bref, nous savons maintenant additionner les polynômes, mais nous voulons aussi pouvoir les multiplier entre eux. Nous serions bien contents de pouvoir écrire ceci : $\left(\sum_{i=0}^{n}a_iX^i\right)\times\left(\sum_{j=0}^{n}b_jX^j\right)=\sum_{k=0}^{2n}\left(a_0b_k+\ldots+a_kb_0\right)X^k=\sum_{k=0}^{2n}\left(\sum_{i=0}^{k}a_ib_{k-i}\right)X^k$, calcul au sein duquel on a simplement regroupé les termes degré par degré. Il ne nous reste plus qu'à forcer le destin.

Définition (Anneau $\mathbb{K}[X]$) Pour tous $P=(a_k)_{k\in\mathbb{N}},Q=(b_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$, on appelle *produit de P et Q* et on note $P\times Q$ ou PQ la suite $\left(\sum_{i=0}^{k}a_ib_{k-i}\right)_{k\in\mathbb{N}}=\left(a_0b_k+\ldots+a_kb_0\right)_{k\in\mathbb{N}}$, qui se trouve être un polynôme.

Le triplet $\left(\mathbb{K}[X],+,\times\right)$ est alors un anneau commutatif d'éléments neutres le polynôme nul 0 pour $+$ et le polynôme constant 1 pour $\times$. En outre, pour tous $P=(a_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$, λP est le polynôme $(\lambda a_k)_{k\in\mathbb{N}}$.

Démonstration Fixons une fois pour toutes $P=(a_k)_{k\in\mathbb{N}},Q=(b_k)_{k\in\mathbb{N}},R=(c_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$.

- **Loi interne :** Il s'agit de montrer que le produit de deux polynômes est bien un polynôme, i.e. une suite PRESQUE NULLE. Notons N un rang à partir duquel $a_k=b_k=0$. Or pour tout $k\geqslant 2N$:
$$\sum_{i=0}^{k}a_ib_{k-i}=\sum_{i=0}^{N-1}a_i\underbrace{b_{k-i}}_{\substack{=0\text{ car}\\k-i>k-N\geqslant N}}+\sum_{i=N}^{k}\underbrace{a_i}_{=0}b_{k-i}=0,\qquad\text{donc en effet } PQ\in\mathbb{K}[X].$$
- **Multiplication par un scalaire :** Soit $\lambda\in\mathbb{K}$. Pour tout $k\in\mathbb{N}$, le coefficient de degré k de λP vaut $\lambda a_k+0.a_{k-1}+\ldots+0.a_0=\lambda a_k$, donc $\lambda P=(\lambda a_k)_{k\in\mathbb{N}}$. En particulier : $1\times P=P$.
- **Commutativité de $\times$:** Pour tout $k\in\mathbb{N}$: $\sum_{i=0}^{k}a_ib_{k-i}\overset{j=k-i}{=}\sum_{j=0}^{k}b_ja_{k-j}$, donc $PQ=QP$.
- **Associativité de $\times$:** Pour tout $k\in\mathbb{N}$, le coefficient de degré k de $(PQ)R$ est :
$$\sum_{i=0}^{k}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)c_{k-i}=\sum_{0\leqslant j\leqslant i\leqslant k}a_jb_{i-j}c_{k-i}=\sum_{j=0}^{k}a_j\left(\sum_{i=j}^{k}b_{i-j}c_{k-i}\right)\overset{l=i-j}{=}\sum_{j=0}^{k}a_j\left(\sum_{l=0}^{k-j}b_lc_{(k-j)-l}\right),$$
donc est égal au coefficient de degré k de $P(QR)$, donc $(PQ)R=P(QR)$.
- **Distributivité de $\times$ sur $+$:** Pour tout $k\in\mathbb{N}$, le coefficient de degré k de $P(Q+R)$ est :
$$\sum_{i=0}^{k}a_i\left(b_{k-i}+c_{k-i}\right)=\sum_{i=0}^{k}a_ib_{k-i}+\sum_{i=0}^{k}a_ic_{k-i},$$
donc est égal au coefficient de degré k de $(PQ)+(PR)$, donc $P(Q+R)=(PQ)+(PR)$. ∎

Et voilà, le temps de la notation polynomiale est enfin arrivé ! Grâce au théorème suivant, les polynômes seront désormais toujours notés comme des polynômes au sens intuitif du terme. Je n'irai pas jusqu'à vous conseiller d'oublier la construction que nous venons d'effectuer — et qui n'est pas terminée — mais nous n'aurons bientôt plus du tout besoin de voir les polynômes comme des suites presque nulles. Ce point de vue nous a seulement permis de fonder proprement le monde des polynômes *formels* — on les qualifie de « formels » pour les distinguer des fonctions polynomiales, sur lesquelles nous reviendrons plus tard.

Théorème **(Notation polynomiale)** Dans $\mathbb{K}[X]$, on choisit de noter X le polynôme $(0,1,0,0,\dots)$.

- Pour tout $k\in\mathbb{N}$: $X^k=(0,\dots,0,1,0,0,\dots)$, polynôme dans lequel le 1 est en position « degré k ».
$$1=(1,0,0,\dots),\qquad X=(0,1,0,0,\dots),\qquad X^2=(0,0,1,0,0,\dots),\qquad X^3=(0,0,0,1,0,0,\dots)\dots$$
- Pour tout $P=(a_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$ non nul de degré n : $P=\sum_{k=0}^{n}a_kX^k$. On peut aussi écrire que $P=\sum_{k=0}^{+\infty}a_kX^k$ et cette écriture est unique. Une telle somme est FINIE contrairement aux apparences car la suite $(a_k)_{k\in\mathbb{N}}$ est presque nulle. Cette notation « infinie » rend de précieux services de rédaction.

Démonstration L'égalité $X^k=(0,\dots,0,1,0,0,\dots)$ pour tout $k\in\mathbb{N}$ se démontre par récurrence. ∎

Attention ! X N'EST PAS UN NOMBRE ! Ôtez-vous une fois pour toutes cette idée de la tête.

Le résultat suivant ne nous est d'aucune utilité pour le moment, mais nous l'utiliserons plus tard dans nos pérégrinations probabilistes et c'est pile poil le bon moment pour le démontrer.

Théorème **(Formule de Vandermonde)** Pour tout $n\in\mathbb{N}$: $\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

Démonstration L'égalité $(X+1)^{2n}=(X+1)^n(X+1)^n$ s'écrit aussi : $\sum_{k=0}^{2n}\binom{2n}{k}X^k=\sum_{i=0}^{n}\binom{n}{i}X^i\times\sum_{j=0}^{n}\binom{n}{j}X^j$.
À gauche, le coefficient de degré n vaut $\binom{2n}{n}$, et il vaut $\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}=\sum_{i=0}^{n}\binom{n}{i}^2$ à droite par définition du produit de deux polynômes. ∎

Théorème **(Addition, multiplication et degré)** Soient $P,Q\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$.

(i) **Degré d'une somme :** $\deg(P+Q)\leqslant\max\{\deg(P),\deg(Q)\}$.
Cette inégalité est une égalité notamment quand $\deg(P)>\deg(Q)$ ou $\deg(Q)>\deg(P)$.

(ii) **Degré d'un produit :** $\deg(PQ)=\deg(P)+\deg(Q)$. En particulier, pour $\lambda\neq0$: $\deg(\lambda P)=\deg(P)$.

Démonstration Le résultat est évident lorsque P ou Q est nul. Supposons-les donc tous deux non nuls et notons m le degré de P et n celui de Q, ainsi que $P=(a_k)_{k\in\mathbb{N}}$, $Q=(b_k)_{k\in\mathbb{N}}$ et $PQ=(c_k)_{k\in\mathbb{N}}$.

(i) Pour tout $k>\max\{m,n\}$: $a_k+b_k=0$, donc $\deg(P+Q)\leqslant\max\{m,n\}=\max\{\deg(P),\deg(Q)\}$.

(ii) Pour commencer : $c_{m+n}=\sum_{i=0}^{m+n}a_ib_{m+n-i}=\sum_{i=0}^{m-1}a_i\overbrace{b_{m+n-i}}^{=0}+a_mb_n+\sum_{i=m+1}^{m+n}\overbrace{a_i}^{=0}b_{m+n-i}=a_mb_n$, donc comme $a_m\neq0$ et $b_n\neq0$, forcément $c_{m+n}\neq0$, donc $\deg(PQ)\geqslant m+n$. Inversement, pour tout $k>m+n$:
$c_k=\sum_{i=0}^{m}a_i\underbrace{b_{k-i}}_{=0}+\sum_{i=m+1}^{k}\underbrace{a_i}_{=0}b_{k-i}=0$, donc $\deg(PQ)\leqslant m+n$. ∎

Théorème **(Intégrité de $\mathbb{K}[X]$)** L'anneau $\mathbb{K}[X]$ est intègre : $\forall P,Q\in\mathbb{K}[X],\ \big(PQ=0\implies P=0\text{ ou }Q=0\big)$.

Démonstration Pour commencer, $\mathbb{K}[X]$ est un anneau non nul. Soient ensuite $P,Q\in\mathbb{K}[X]$. Si $PQ=0$: $\deg(P)+\deg(Q)=\deg(PQ)=-\infty$, donc $\deg(P)$ ou $\deg(Q)$ vaut $-\infty$, autrement dit P ou Q est nul. ∎

Ce résultat serait nettement plus difficile à prouver si on travaillait avec des fonctions polynomiales et non avec des polynômes. En effet, si $P(x)Q(x)=0$ pour tout $x\in\mathbb{R}$, alors en tout point l'une des fonctions P et Q s'annule, mais qui nous dit que l'une des deux s'annule tout le temps ? Rien a priori.

Définition-théorème **(Composition des polynômes)**

- **Composée :** Soient $P=\sum_{k=0}^{+\infty}a_kX^k, Q\in\mathbb{K}[X]$. On appelle *composée de Q suivie de P* le polynôme $P\circ Q=\sum_{k=0}^{+\infty}a_kQ^k$.
- **Degré d'une composée :** Si Q n'est pas constant : $\deg(P\circ Q)=\deg(P)\times\deg(Q)$.

Démonstration On suppose Q non constant et on pose $m=\deg(P)$. Par produit : $\deg\left(Q^k\right)=k\deg(Q)$ pour tout $k\in[\![0,m]\!]$, donc comme $\deg(Q)\geqslant 1$, la suite $\left(\deg\left(Q^k\right)\right)_{0\leqslant k\leqslant m}$ est strictement croissante.

Finalement, par somme : $\deg(P\circ Q)=\deg\left(\sum_{k=0}^{m}a_kQ^k\right)\overset{a_m\neq 0}{=}\deg\left(Q^m\right)=m\deg(Q)=\deg(P)\times\deg(Q)$. ∎

Définition **(Dérivation des polynômes)** Soit $P=\sum_{k=0}^{+\infty}a_kX^k\in\mathbb{K}[X]$.

- **Polynôme dérivé :** Le polynôme $P'=\sum_{k=0}^{+\infty}ka_kX^{k-1}$ est appelé le *polynôme dérivé de P* — avec par convention $0\times X^{-1}=0$ pour $k=0$, fausse apparition de X^{-1}.
- **Polynômes dérivés successifs :** On définit pour tout $n\in\mathbb{N}$ le $n^{\text{ème}}$ *polynôme dérivé de P*, noté $P^{(n)}$. On pose pour cela $P^{(0)}=P$ et pour tout $n\in\mathbb{N}$: $P^{(n+1)}=\left(P^{(n)}\right)'$. Pour $n=2$ et $n=3$, on préfère les notations P'' et P''' aux notations $P^{(2)}$ et $P^{(3)}$.

Exemple Pour $P=8X^3-5X^2+3X+1$: $P'=24X^2-10X+3$, $P''=48X-10$, $P'''=48$ et $P^{(4)}=0$.

Théorème **(Propriétés de la dérivation des polynômes)** Soient $P,Q\in\mathbb{K}[X]$ et $n\in\mathbb{N}$.

(i) **Degré :** Si $\deg(P)\geqslant n$: $\deg\left(P^{(n)}\right)=\deg(P)-n$, et si au contraire $\deg(P)<n$: $P^{(n)}=0$.

(ii) **Somme :** $(P+Q)^{(n)}=P^{(n)}+Q^{(n)}$.

(iii) **Produit :** $(PQ)'=P'Q+PQ'$. Plus généralement : $(PQ)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}$ *(formule de Leibniz)*.

Ce sont des DÉRIVÉES, pas des puissances.

(iv) **Composition :** $(P\circ Q)'=Q'\times P'\circ Q$.

Démonstration Introduisons les coefficients de P et Q : $P=\sum_{k=0}^{+\infty}a_kX^k$ et $Q=\sum_{k=0}^{+\infty}b_kX^k$.

(i) Posons $d=\deg(P)$. Si $d\leqslant 0$: $P'=0$. Si au contraire $d\geqslant 1$: $P'=\sum_{k=0}^{d}ka_kX^{k-1}$ avec $da_d\neq 0$, donc $\deg(P')=d-1$. Au-delà, récurrence !

(iii) Montrons que $(PQ)'=P'Q+PQ'$. Soit $k\in\mathbb{N}$. Le coefficient de degré k de $(PQ)'$ vaut $(k+1)\sum_{i=0}^{k+1}a_ib_{k+1-i}$ et celui de $P'Q+PQ'$ vaut $\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j}+\sum_{i=0}^{k}a_i(k-i+1)b_{k-i+1}$. Ces coefficients sont égaux car :

$$\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j}+\sum_{i=0}^{k}a_i(k-i+1)b_{k-i+1}\overset{i=j+1}{=}\sum_{i=1}^{k+1}ia_ib_{k+1-i}+\sum_{i=0}^{k}a_i(k-i+1)b_{k-i+1}$$
$$=\sum_{i=0}^{k+1}ia_ib_{k+1-i}+\sum_{i=0}^{k+1}a_i(k-i+1)b_{k-i+1}=\sum_{i=0}^{k+1}\left(ia_ib_{k+1-i}+a_i(k-i+1)b_{k+1-i}\right)=(k+1)\sum_{i=0}^{k+1}a_ib_{k+1-i}.$$

La formule de Leibniz s'en déduit par récurrence sur n. **Initialisation :** Pour $n=0$, rien à faire !

Hérédité : Soit $n\in\mathbb{N}$. Faisons l'hypothèse que la formule de Leibniz : $(PQ)^{(n)}=\dots$ est vraie pour tous $P,Q\in\mathbb{K}[X]$. Alors pour tous $P,Q\in\mathbb{K}[X]$.

$$(PQ)^{(n+1)}=\left((PQ)'\right)^{(n)}=(P'Q+PQ')^{(n)}\overset{\text{(ii)}}{=}(P'Q)^{(n)}+(PQ')^{(n)}\overset{\text{HDR}}{=}\sum_{k=0}^{n}\binom{n}{k}(P')^{(k)}Q^{(n-k)}+\sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}(Q')^{(n-k')}$$
$$=\sum_{k=0}^{n}\binom{n}{k}P^{(k+1)}Q^{(n-k)}+\sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}Q^{(n+1-k')}\overset{l=k+1}{=}\sum_{l=1}^{n+1}\binom{n}{l-1}P^{(l)}Q^{(n+1-l)}+\sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}Q^{(n+1-k')}$$
$$=P^{(n+1)}Q^{(0)}+\sum_{k=1}^{n}\binom{n}{k-1}P^{(k)}Q^{(n+1-k)}+\sum_{k=1}^{n}\binom{n}{k}P^{(k)}Q^{(n+1-k)}+P^{(0)}Q^{(n+1)}$$

$$= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)P^{(k)}Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} \qquad \text{— tiens, la formule de Pascal !}$$

$$= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} = \sum_{k=0}^{n+1}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)}.$$

(iv) Par définition $P\circ Q = \sum_{k=0}^{+\infty} a_k Q^k$, donc $(P\circ Q)' = \sum_{k=0}^{+\infty} a_k\left(Q^k\right)'$. Ensuite $\left(Q^k\right)' = kQ'Q^{k-1}$ pour tout $k\in\mathbb{N}$ par récurrence à partir de (iii), donc $(P\circ Q)' = \sum_{k=0}^{+\infty} a_k \times kQ'Q^{k-1} = Q'\times P'\circ Q$. ∎

Notre construction des polynômes ne saurait s'achever sans un rapide retour à la notion de *fonction polynomiale*, dont nous reparlerons aussi plus loin.

Définition-théorème **(Évaluation polynomiale, fonction polynomiale)**

- **Évaluation :** Pour tous $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$ et $\lambda\in\mathbb{K}$, on pose $P(\lambda) = \sum_{k=0}^{+\infty} a_k\lambda^k$ — c'est un élément de $\mathbb{K}$.
- **Fonction polynomiale :** Pour tout $P\in\mathbb{K}[X]$, la fonction $x\longmapsto P(x)$ de $\mathbb{K}$ dans $\mathbb{K}$ est appelée la *fonction polynomiale associée à* P. On la note souvent P par abus et parfois $\widetilde{P}$ quand on veut la distinguer du polynôme P.

  Pour tous $P,Q\in\mathbb{K}[X]$: $\widetilde{P+Q} = \widetilde{P}+\widetilde{Q}$, $\widetilde{PQ} = \widetilde{P}\,\widetilde{Q}$, $\widetilde{P\circ Q} = \widetilde{P}\circ\widetilde{Q}$ et $\widetilde{P'} = \widetilde{P}'$.

Nous en omettrons la preuve, mais la dernière assertion n'est pas une évidence. Nous disposons sur $\mathbb{R}[X]$ et $\mathbb{R}^{\mathbb{R}}$ de notions différentes d'addition, multiplication, composition et dérivation. Dans la formule $\widetilde{P\circ Q} = \widetilde{P}\circ\widetilde{Q}$ par exemple, ce ne sont pas les mêmes « $\circ$ » qu'on trouve à gauche et à droite, et dans la formule $\widetilde{P'} = \widetilde{P}'$, la dérivée P' est une dérivée formelle alors que la dérivée $\widetilde{P}'$ est la dérivée d'une fonction définie comme limite d'un taux d'acroissement.

Sachant que $\widetilde{1}$ est la fonction constante $x\longmapsto 1$ — élément neutre de $\mathbb{K}^{\mathbb{K}}$ — l'application $P\longmapsto\widetilde{P}$ s'avère être un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$.

Attention ! X N'EST PAS UN NOMBRE ! On ne dit pas « Posons $X=1$ », mais « Évaluons en 1 ».

2 Divisibilité et division polynomiales

2.1 Relation de divisibilité

Définition **(Divisibilité, diviseur, multiple)** Soient $A,B\in\mathbb{K}[X]$. On dit que A *divise* B, ou que A est un *diviseur de* B, ou que B est *divisible par* A, ou que B est un *multiple de* A, s'il existe $P\in\mathbb{K}[X]$ pour lequel $B=AP$. Cette relation se note $A\mid B$.

Exemple Le polynôme X^2+3X+2 est divisible par $X+1$ car $X^2+3X+2 = (X+1)(X+2)$.

On peut définir une notion de divisibilité dans tout anneau quel qu'il soit — dans $\mathbb{Z}$ et maintenant $\mathbb{K}[X]$, mais bien au-delà. La divisibilité est en un sens ce qui différencie les anneaux les uns des autres et le point de départ de l'*arithmétique* en général. La très grande proximité des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ justifie que nous omettions ci-après certaines preuves qui ressemblent à s'y méprendre aux preuves du chapitre « Arithmétique des entiers relatifs ».

Théorème **(Propriétés de la relation de divisibilité)** Soient $A,B,C,D\in\mathbb{K}[X]$.

- **Relation d'ordre :** La relation de divisibilité $\mid$ est réflexive et transitive sur $\mathbb{K}[X]$, c'est même une relation d'ordre sur l'ensemble des polynômes UNITAIRES OU NULS de $\mathbb{K}[X]$. Elle est en revanche seulement réflexive et transitive sur $\mathbb{K}[X]$ car pour tous $A,B\in\mathbb{K}[X]$:

  $$A\mid B \quad\text{et}\quad B\mid A \iff \exists\lambda\in\mathbb{K}^*,\ A=\lambda B.$$

  On dit alors que A et B sont *associés* (*sur* $\mathbb{K}$).
- **Combinaisons linéaires :** Si $D\mid A$ et $D\mid B$, alors $D\mid (AU+BV)$ pour tous $U,V\in\mathbb{K}[X]$.
- **Produit :** Si $A\mid B$ et $C\mid D$, alors $AC\mid BD$, et en particulier $A^k\mid B^k$ pour tout $k\in\mathbb{N}$.

Démonstration Pour le défaut d'antisymétrie, si $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$: $B = \frac{1}{\lambda} A$, donc $A \mid B$ et $B \mid A$. Réciproquement, faisons l'hypothèse que $A \mid B$ et $B \mid A$. Il existe alors deux polynômes $P, Q \in \mathbb{K}[X]$ pour lesquels $A = BP$ et $B = AQ$, et ainsi $A = APQ$. Deux cas se présentent alors.

— Si $A = 0$, alors $B = AQ = 0$, donc $A = \lambda B$ pour $\lambda = 1$.

— Si au contraire $A \neq 0$, alors $PQ = 1$ par intégrité de $\mathbb{K}[X]$, donc P et Q sont non nuls, donc de degrés entiers. Les inégalités : $0 \leqslant \deg(P) \leqslant \deg(P) + \deg(Q) = \deg(PQ) = \deg(1) = 0$ montrent alors que $\deg(P) = 0$, i.e. que P est une constante non nulle λ. Conclusion : $A = \lambda B$. ∎

2.2 Division euclidienne

Nous pratiquons la division euclidienne des polynômes depuis le chapitre « Introduction à la décomposition en éléments simples », mais nous n'avions rien démontré alors, il est temps de le faire.

Théorème (Division euclidienne) Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un et un seul couple de polynômes $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ pour lequel : $A = BQ + R$ et $\deg(R) < \deg(B)$. On appelle A le *dividende* de la division euclidienne de A par B, B son *diviseur*, Q son *quotient* et R son *reste*.

Démonstration

- **Existence :** Notons b le degré de B et $\beta \neq 0$ son coefficient dominant. Si B divise A, alors $A = BQ$ pour un certain $Q \in \mathbb{K}[X]$ et on peut poser $R = 0$. Supposons maintenant que B ne divise pas A. L'ensemble $\mathscr{D} = \left\{\deg(A - BK) \mid K \in \mathbb{K}[X]\right\}$ est alors une partie non vide de $\mathbb{N}$ — valeur $-\infty$ exclue par hypothèse — donc possède un plus petit élément r. Notons $Q \in \mathbb{K}[X]$ un polynôme pour lequel $\deg(A - BQ) = r$, puis posons $R = A - BQ$ et notons ρ le coefficient dominant de R. Est-il vrai que $\deg(R) < \deg(B)$?

  Supposons par l'absurde que $r \geqslant b$. Alors $\deg\left(R - \frac{\rho}{\beta} X^{r-b} B\right) < r$ car la soustraction de $\frac{\rho}{\beta} X^{r-b} B$ tue le terme dominant ρX^r de R. Or $\deg\left(R - \frac{\rho}{\beta} X^{r-b} B\right) = \deg(A - BK) \in \mathscr{D}$ si l'on pose $K = Q + \frac{\rho}{\beta} X^{r-b}$. La minimalité de r est ainsi contredite. Comme voulu $r < b$.
- **Unicité :** Soient (Q_1, R_1) et (Q_2, R_2) deux couples de la division euclidienne de A par B. Par définition $B(Q_1 - Q_2) = R_2 - R_1$. Si $Q_1 \neq Q_2$, alors $\deg(Q_1 - Q_2) \geqslant 0$, donc $\deg\big(B(Q_1 - Q_2)\big) \geqslant \deg(B)$ alors que $\deg(R_2 - R_1) < \deg(B)$ par définition de R_1 et R_2 — contradiction. Conclusion : $Q_1 = Q_2$, et en retour $R_1 = A - BQ_1 = A - BQ_2 = R_2$. ∎

3 Racines d'un polynôme

3.1 Racines et multiplicités

Théorème (Division euclidienne par $X - \lambda$) Soient $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Le reste de la division euclidienne de P par $X - \lambda$ est $P(\lambda)$.

Démonstration La division de P par $X - \lambda$ s'écrit $P = (X - \lambda)Q + R$ pour certains $Q, R \in \mathbb{K}[X]$ avec $\deg(R) < 1$, donc en fait R est un polynôme constant. Évaluons en λ : $P(\lambda) = (\lambda - \lambda)Q(\lambda) + R(\lambda) = R$. ∎

De ce théorème découle directement la double définition suivante :

Définition (Racine) Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On dit que λ est une *racine de P (dans $\mathbb{K}$)* si l'une des deux assertions équivalentes suivantes est vraie : $P(\lambda) = 0$ ou bien : P est divisible par $X - \lambda$.

✖ **Attention !** La précision « racine DANS $\mathbb{K}$ » n'est pas superflue. Le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, mais il en a deux dans $\mathbb{C}$, à savoir i et −i.

Via la notion de racine, on ramène souvent les PROBLÈMES DE DIVISIBILITÉ à des PROBLÈMES D'ÉVALUATION — et vice versa — comme l'illustre l'exemple suivant.

Exemple Pour tout $n \in \mathbb{N}$, le reste de la division euclidienne de X^n par X^2-3X+2 vaut $(2^n-1)X-(2^n-2)$.

Démonstration Soit $n \in \mathbb{N}$. La division euclidienne de X^n par X^2-3X+2 s'écrit $X^n = (X-1)(X-2)Q+aX+b$ pour certains $Q \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$. Évaluons en 1 : $1 = a+b$, puis en 2 : $2^n = 2a+b$. Après calcul : $a = 2^n-1$ et $b = 2-2^n$.

Définition (Multiplicité d'une racine) Soient $P \in \mathbb{K}[X]$ NON NUL et $\lambda \in \mathbb{K}$.

- L'ensemble $\left\{k \in \mathbb{N} \mid (X-\lambda)^k \text{ divise } P\right\}$ possède un plus grand élément m appelé la *multiplicité de λ dans P*. On dit souvent pour résumer que m est la plus grande puissance de $X-\lambda$ qui divise P.
  En particulier, dire que λ N'EST PAS racine de P, c'est dire que λ a pour multiplicité 0 dans P. Une racine est dite *simple* si elle est de multiplicité 1, *double* si elle est de multiplicité 2, etc.
- Plus concrètement, m est caractérisé par les deux propositions suivantes, équivalentes :
  — P est divisible par $(X-\lambda)^m$ mais PAS par $(X-\lambda)^{m+1}$.
  — Il existe $Q \in \mathbb{K}[X]$ pour lequel $P = (X-\lambda)^m Q$ et $Q(\lambda) \neq 0$.

Démonstration Pour montrer que l'ensemble $\mathscr{M} = \left\{k \in \mathbb{N} \mid (X-\lambda)^k \text{ divise } P\right\}$ possède un plus grand élément, nous allons montrer que c'est une partie non vide majorée de $\mathbb{N}$. Or déjà, $\mathscr{M}$ contient 0. Montrons ensuite que $\deg(P)$ majore $\mathscr{M}$. Pour tout $k \in \mathscr{M}$: $P = (X-\lambda)^k Q$ pour un certain $Q \in \mathbb{K}[X]$ avec $Q \neq 0$ car $P \neq 0$. En particulier $\deg(Q) \geqslant 0$, donc $k \leqslant \deg(Q)+k = \deg(P)$.

Théorème (Formule de Taylor polynomiale) Pour tous $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$: $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k$.
En particulier, pour tout $k \in \mathbb{N}$, le coefficient de degré k de P est $\frac{P^{(k)}(0)}{k!}$.

Démonstration

- **Cas où $\lambda = 0$:** En notant $P = \sum_{i=0}^{+\infty} a_i X^i$, dérivons k fois pour tout $k \in \mathbb{N}$: $P^{(k)} = \sum_{i=k}^{+\infty} a_i \frac{i!}{(i-k)!} X^{i-k}$, puis évaluons en 0 : $P^{(k)}(0) = \underbrace{a_k\, k!}_{i=k}$. Aussitôt $a_k = \frac{P^{(k)}(0)}{k!}$, donc $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} X^k$.
- **Cas général :** Posons $Q = P(X+\lambda)$. Pour tout $k \in \mathbb{N}$: $Q^{(k)} = P^{(k)}(X+\lambda)$, donc :
$$Q = \sum_{k=0}^{+\infty} \frac{Q^{(k)}(0)}{k!} X^k = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} X^k, \quad \text{et on compose à droite par } X-\lambda \text{ pour terminer.}$$

Théorème (Utilisation des dérivées successives pour le calcul d'une multiplicité) Soient $P \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$ et $m \in \mathbb{N}$.

(i) λ est de multiplicité m dans P si et seulement si $P^{(i)}(\lambda) = 0$ pour tout $i \in [\![0, m-1]\!]$ MAIS $P^{(m)}(\lambda) \neq 0$.

(ii) Si λ est de multiplicité $m \geqslant 1$ dans P, λ est de multiplicité $m-1$ dans P'.

Démonstration Démontrons l'assertion (i), dont l'assertion (ii) est une simple conséquence. L'air de rien, la formule de Taylor nous fournit facilement la division euclidienne de P par $(X-\lambda)^m$:
$$P \overset{\text{Taylor}}{=} \sum_{i=0}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i = (X-\lambda)^m \sum_{i=m}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^{i-m} + \underbrace{\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i}_{\text{Degré strictement inférieur à } m}.$$
On en tire les équivalences suivantes :
$$\begin{aligned} \lambda \text{ est de multiplicité au moins } m \text{ dans } P &\iff (X-\lambda)^m \text{ divise } P \iff \sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i = 0 \\ &\iff \sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!} X^i = 0 \quad \text{après composition à droite par } X+\lambda \\ &\iff \forall i \in [\![0, m-1]\!], \quad P^{(i)}(\lambda) = 0. \end{aligned}$$
Or pour la même raison : λ est de multiplicité au moins $m+1$ dans $P \iff \forall i \in [\![0, m]\!], \quad P^{(i)}(\lambda) = 0$. Il en découle que λ est de multiplicité EXACTEMENT m dans P si et seulement si $P^{(i)}(\lambda) = 0$ pour tout $i \in [\![0, m-1]\!]$ mais $P^{(m)}(\lambda) \neq 0$.

Exemple La multiplicité de 1 dans $P = X^4 + 3X^3 - 3X^2 - 7X + 6$ est égale à 2.

Démonstration Déjà : $P(1) = 1+3-3-7+6 = 0$. Ensuite : $P' = 4X^3 + 9X^2 - 6X - 7$ donc $P'(1) = 0$. Enfin : $P'' = 12X^2 + 18X - 6$ donc $P''(1) = 24 \neq 0$.

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Nous avons déjà vu de quelle manière les racines de B peuvent être utilisées pour calculer le reste de la division euclidienne de A par B. Si par exemple $B = (X-2)^3(X+3)$, la division euclidienne de A par B s'écrit $A = (X-2)^3(X+3)Q + aX^3 + bX^2 + cX + d$ pour certains $Q \in \mathbb{R}[X]$ et $a, b, c, d \in \mathbb{R}$. On n'obtient hélas que deux équations en évaluant en 2 et -3, mais on va en obtenir deux de plus en exploitant la multiplicité de 2 dans B. Et comment on fait ? On dérive ! La multiplicité de 2 est au moins 3 dans $BQ = (X-2)^3(X+3)Q$, donc au moins 2 dans $(BQ)'$ et au moins 1 dans $(BQ)''$. On en tire deux nouvelles équations $A'(2) = 12a + 4b + c$ et $A''(2) = 12a + 2b$, et de là on conclut en résolvant un système linéaire 4×4.

Exemple Pour tout $n \in \mathbb{N}^*$, le reste de la division euclidienne de X^n par $X(X-1)^2$ vaut $(n-1)X^2 - (n-2)X$.

Démonstration La division euclidienne étudiée s'écrit $X^n = X(X-1)^2Q + aX^2 + bX + c$ pour certains $Q \in \mathbb{R}[X]$ et $a, b, c \in \mathbb{R}$. Évaluons en 0 : $c = 0$, puis en 1 : $a + b + c = 1$, ou encore $a + b = 1$. Il nous manque une équation. Dérivons puis évaluons en 1 pour exploiter la multiplicité 2 de la racine 1 : $2a + b = n$. Après calcul : $a = n - 1$, $b = 2 - n$ et $c = 0$.

Théorème (Racines complexes d'un polynôme réel) Soient $P \in \mathbb{R}[X]$ — à coefficients réels, donc — et $\lambda \in \mathbb{C}$. Alors λ et $\overline{\lambda}$ ont la même multiplicité dans P.

Démonstration Comme $P = \sum_{k=0}^{+\infty} a_k X^k$ est à coefficients $(a_k)_{k\in\mathbb{N}}$ **RÉELS**, pour tout $i \in \mathbb{N}$:

$$\overline{P^{(i)}(\lambda)} = \overline{\sum_{k=i}^{+\infty} a_k \times \frac{k!}{(k-i)!}\lambda^{k-i}} = \sum_{k=i}^{+\infty} a_k \times \frac{k!}{(k-i)!}\overline{\lambda}^{k-i} = P^{(i)}(\overline{\lambda}),$$

donc en effet, λ et $\overline{\lambda}$ ont la même multiplicité dans P d'après la caractérisation précédente.

3.2 Nombre maximal de racines

Théorème (Factorisation « par les racines ») Soient $P \in \mathbb{K}[X]$ **NON NUL** et $\lambda_1, \dots, \lambda_r$ des racines distinctes de P de multiplicités respectives $m_1, \dots, m_r$. Alors $(X-\lambda_1)^{m_1} \dots (X-\lambda_r)^{m_r}$ divise P. En particulier $m_1 + \dots + m_r \leqslant \deg(P)$.

Démonstration Montrons par récurrence que pour tout $k \in [\![1, r]\!]$, $(X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k}$ divise P.

Initialisation : λ_1 est racine de P de multiplicité m_1, donc $(X-\lambda_1)^{m_1}$ divise P.

Hérédité : Soit $k \in [\![1, r-1]\!]$. Faisons l'hypothèse que $(X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k}$ divise P.

- Dans ces conditions, $P = (X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k} A$ pour un certain $A \in \mathbb{K}[X]$.
- Ensuite, si on note α la multiplicité de λ_{k+1} dans A, $A = (X-\lambda_{k+1})^\alpha B$ pour un certain $B \in \mathbb{K}[X]$ avec $B(\lambda_{k+1}) \neq 0$. Et comme $(X-\lambda_{k+1})^\alpha$ divise A, il divise aussi P, donc $\alpha \leqslant m_{k+1}$.
- Enfin, $P = (X-\lambda_{k+1})^{m_{k+1}} C$ pour un certain $C \in \mathbb{K}[X]$ avec $C(\lambda_{k+1}) \neq 0$.

Il découle de ces trois points que : $(X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k}(X-\lambda_{k+1})^\alpha B = (X-\lambda_{k+1})^{m_{k+1}} C$. Divisons cette égalité par $(X-\lambda_{k+1})^\alpha$ grâce à l'intégrité de $\mathbb{K}[X]$: $(X-\lambda_1)^{m_1} \dots (X-\lambda_k)^{m_k} B = (X-\lambda_{k+1})^{m_{k+1}-\alpha} C$. Le polynôme de gauche n'admet pas λ_{k+1} pour racine, donc celui de droite non plus, donc $\alpha = m_{k+1}$. Conclusion : $(X-\lambda_{k+1})^{m_{k+1}}$ divise A, donc $(X-\lambda_1)^{m_1} \dots (X-\lambda_{k+1})^{m_{k+1}}$ divise P.

Exemple À quelle condition nécessaire et suffisante sur $n \in \mathbb{N}$ le polynôme X^2+1 divise-t-il X^n+1 ? Réponse : $n \equiv 2\,[4]$.

Démonstration Pour tout $n \in \mathbb{N}$:

$$\begin{aligned}
&X^2+1 \text{ divise } X^n+1 && \iff && \mathrm{i} \text{ et } -\mathrm{i} \text{ sont racines de } X^n+1\\
&\iff && \mathrm{i} \text{ est racine de } X^n+1 && \text{car } X^n+1 \text{ est à coefficients réels}\\
&\iff && \mathrm{i}^n + 1 = 0 && \iff \quad \mathrm{e}^{\frac{\mathrm{i}n\pi}{2}} = \mathrm{e}^{\mathrm{i}\pi}\\
&\iff && \frac{n\pi}{2} \equiv \pi\,[2\pi] && \iff \quad n \equiv 2\,[4].
\end{aligned}$$

Dans cette chaîne d'équivalences, le théorème de factorisation « par les racines » justifie l'implication :

$$\mathrm{i} \text{ et } -\mathrm{i} \text{ sont racines de } X^n+1 \quad \Longrightarrow \quad X^2+1 \text{ divise } X^n+1.$$

Exemple Le polynôme $(X-1)^4X^2(X+2)$ possède en tout trois racines distinctes — 1 de multiplicité 4, 0 double et -2 simple. On dit en revanche qu'il possède 7 RACINES COMPTÉES AVEC MULTIPLICITÉ, car $7=4+2+1$.

Théorème (Nombre maximal de racines comptées avec multiplicité)

- Un polynôme NON NUL P possède au plus $\deg(P)$ racines COMPTÉES AVEC MULTIPLICITÉ.
- En particulier, seul le polynôme nul possède une infinité de racines.

Attention ! En dépit des apparences, ce théorème est l'un des plus importants du chapitre !

Un polynôme de degré n ne possède pas forcément n racines comptées avec multiplicité. Nous verrons au prochain paragraphe que c'est le cas si $\mathbb{K}=\mathbb{C}$, mais pas si $\mathbb{K}=\mathbb{R}$. Par exemple, X^2+1 est réel de degré 2 mais n'a pas de racine réelle.

Exemple Soit $P\in\mathbb{R}[X]$. On suppose que $P(n)=n^3-n^2+1$ pour tout $n\in\mathbb{N}$. Alors $P=X^3-X^2+1$, donc en fait $P(z)=z^3-z^2+1$ pour tout $z\in\mathbb{C}$!

Démonstration On connaît ici P SEULEMENT en les entiers naturels et cela ne nous permet pas a priori d'affirmer que $P=X^3-X^2+1$, ni que $P(z)=z^3-z^2+1$ pour tout $z\in\mathbb{C}$. Il est pourtant facile d'obtenir ces résultats grâce à la notion de RACINE. En effet, le polynôme $P-X^3+X^2-1$ admet par hypothèse tout entier naturel pour racine, donc possède une infinité de racines, donc est nul. Comme voulu $P=X^3-X^2+1$.

On le voit bien sur cet exemple, le théorème qui précède est un théorème de « désévaluation » (néologisme pratique). Évaluer, c'est passer d'une égalité polynomiale à une égalité de nombres réels ou complexes. Désévaluer, c'est le contraire — remonter d'une collection d'égalités de nombres à une égalité polynomiale. En d'autres termes, quand un polynôme P est défini par certaines de ses VALEURS, il est souvent fructueux d'interpréter cette hypothèse sur les valeurs de P en termes de RACINES d'un nouveau polynôme Q. Quand ce polynôme Q a trop de racines, il est forcément nul et on en tire souvent de précieux renseignements sur P. Les deux exemples qui suivent illustrent cette idée.

Exemple Il n'existe pas de polynôme $P\in\mathbb{R}[X]$ pour lequel $P(n)=\sqrt[3]{n^2+1}$ pour tout $n\in\mathbb{N}$.

Démonstration Supposons par l'absurde qu'un tel polynôme P existe. Le polynôme P^3-X^2-1 admet alors tout entier naturel pour racine, donc possède ainsi une infinité de racines, donc est nul, de sorte que $P^3=X^2+1$. En particulier $3\deg(P)=2$, donc $\deg(P)=\dfrac{2}{3}$ — contradiction.

Exemple Soit $P\in\mathbb{R}[X]$. On suppose que P est de degré n entier et que $P(k)=\dfrac{1}{k}$ pour tout $k\in[\![1,n+1]\!]$.
Dans ces conditions : $P(-1)=n+1$.

Démonstration

- **Analyse des hypothèses :** Le polynôme $XP(X)-1$ admet $1,2,\dots,n+1$ pour racines, soit déjà $n+1$ racines distinctes, or il est justement de degré $n+1$, donc $XP(X)-1=\lambda\prod_{k=1}^{n+1}(X-k)$ pour un certain $\lambda\in\mathbb{R}^*$.
  Évaluons en 0 : $-1=\lambda\prod_{k=1}^{n+1}(-k)$, i.e. $\lambda=\dfrac{(-1)^n}{(n+1)!}$. Enfin : $XP(X)=1+\dfrac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(X-k)$.
- **Calcul de $P(-1)$:** Évaluons simplement ce résultat en -1 :
$$-P(-1)=1+\frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}\big(-(k+1)\big)=1+\frac{(-1)^n}{(n+1)!}\times(-1)^{n+1}(n+2)!=1-(n+2),\qquad\text{donc } P(-1)=n+1.$$

Théorème (Identification polynôme/fonction polynomiale) Pour tous $P,Q\in\mathbb{K}[X]$, si les fonctions polynomiales $\widetilde{P}$ et $\widetilde{Q}$ sont égales, alors les polynômes P et Q eux-mêmes le sont, autrement dit leurs coefficients coïncident.

Démonstration Il s'agit de montrer que le morphisme d'anneaux $P\overset{f}{\longmapsto}\widetilde{P}$ de $\mathbb{K}[X]$ dans $\mathbb{K}^{\mathbb{K}}$ est injectif. Soit $P\in\operatorname{Ker}f$. La fonction $f(P)=\widetilde{P}$ est identiquement nulle sur $\mathbb{K}$, donc tout élément de $\mathbb{K}$ est racine de P. Le corps $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$) étant infini, P possède ainsi une INFINITÉ de racines, donc est nul et c'est fini.

3.3 Polynômes scindés et théorème de d'Alembert-Gauss

Définition **(Polynôme scindé)** Soit $P \in \mathbb{K}[X]$. On dit que P est *scindé* (*sur* $\mathbb{K}$) s'il n'est pas constant et possède exactement $\deg(P)$ racines (dans $\mathbb{K}$) comptées avec multiplicité.

Il est équivalent d'exiger que P puisse être écrit sous la forme $P = a\prod_{k=1}^{r}(X-\lambda_k)^{m_k}$ où a est le coefficient dominant de P, $\lambda_1, \dots, \lambda_r$ ses racines distinctes dans $\mathbb{K}$ et $m_1, \dots, m_r$ leurs multiplicités respectives.

Forme scindée = 3 informations (racines, multiplicités, coefficient dominant)

Attention ! La précision « scindé sur $\mathbb{K}$ » n'est pas superflue car un polynôme peut avoir des racines complexes mais aucune réelle. Le polynôme $X^2+1 = (X+\mathrm{i})(X-\mathrm{i})$ est ainsi scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

Exemple Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$: $X^n - 1 = \prod_{\omega \in \mathbb{U}_n}(X-\omega) = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)$.

Démonstration Le polynôme X^n-1 n'est pas constant et admet les n nombres $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$ pour racines distinctes, k décrivant $[\![0, n-1]\!]$. Comme il possède au plus n racines comptées avec multiplicité, il en possède forcément exactement n, donc est scindé sur $\mathbb{C}$.

Exemple Le polynôme X^3+27 est scindé sur $\mathbb{C}$ et sa forme scindée vaut : $X^3 + 27 = (X-3)\left(X - 3\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}\right)\left(X - 3\mathrm{e}^{-\frac{\mathrm{i}\pi}{3}}\right)$.

Démonstration Pour tout $r \in \mathbb{C}$:
$$r^3 + 27 = 0 \iff r^3 = -27 = \left(3\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}\right)^3 \iff \exists k \in [\![0,2]\!],\quad r = 3\mathrm{e}^{\frac{\mathrm{i}\pi}{3}+\frac{2\mathrm{i}k\pi}{3}}.$$
Les racines complexes de X^3+27 sont donc : $3\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}$ $(k=0)$, $3\mathrm{e}^{\mathrm{i}\pi} = -3$ $(k=1)$ et $3\mathrm{e}^{\frac{5\mathrm{i}\pi}{3}} = 3\mathrm{e}^{-\frac{\mathrm{i}\pi}{3}}$ $(k=2)$. Ces trois racines sont distinctes et X^3+27 est de degré 3, donc est scindé sur $\mathbb{C}$ à racines simples — de coefficient dominant 1.

Tout polynôme possède-t-il une racine ? Question essentielle s'il en est, mais à laquelle nous n'avons pas encore répondu. La réponse affirmative suivante est un théorème majeur des mathématiques et l'un des rares théorèmes que nous ne démontrerons pas cette année. Les curieux en trouveront tout de même une preuve en fin de chapitre.

Théorème **(Théorème de d'Alembert-Gauss)**
Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine **complexe**. A fortiori, tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Démonstration Une fois qu'on a prouvé la première partie du théorème, le caractère scindé sur $\mathbb{C}$ de tout polynôme non constant de $\mathbb{C}[X]$ se démontre aisément par récurrence. ∎

Attention ! Le théorème est faux sur $\mathbb{R}$ — un polynôme non constant de $\mathbb{R}[X]$ peut ne pas avoir de racine **réelle**, par exemple le polynôme X^2+1.

Les multiplicités de racines sont aux polynômes ce que les valuations p-adiques sont aux entiers et le critère de divisibilité qui suit se démontre dans $\mathbb{C}[X]$ comme son analogue dans $\mathbb{Z}$.

Théorème **(Divisibilité dans $\mathbb{C}[X]$ et racines)** Soient $A, B \in \mathbb{C}[X]$ non nuls. Alors A divise B si et seulement si pour tout $\lambda \in \mathbb{C}$, la multiplicité de λ dans A est inférieure à sa multiplicité dans B.

3.4 Relations coefficients-racines

Le prochain théorème est rebutant au premier abord, commençons par deux cas simples. On travaille ci-dessous avec des polynômes non constants de $\mathbb{C}[X]$, donc avec des polynômes scindés sur $\mathbb{C}$ d'après le théorème de d'Alembert-Gauss.

- **Polynômes de degré 2 :** Soit $P = a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$ de racines λ_1 et λ_2 comptées avec multiplicité. Alors : $P = a_2(X-\lambda_1)(X-\lambda_2) = a_2X^2 - a_2(\lambda_1+\lambda_2)X + a_2\lambda_1\lambda_2$, donc après identification : $\lambda_1 + \lambda_2 = -\dfrac{a_1}{a_2}$ (somme des racines) et $\lambda_1\lambda_2 = \dfrac{a_0}{a_2}$ (produit des racines).

- **Polynômes de degré 3 :** Soit $P = a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$ de racines $\lambda_1, \lambda_2, \lambda_3$ comptées avec multiplicité. Alors : $P = a_3(X-\lambda_1)(X-\lambda_2)(X-\lambda_3) = a_3X^3 - a_3\big(\lambda_1+\lambda_2+\lambda_3\big)X^2 + a_3\big(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3\big)X - a_3\lambda_1\lambda_2\lambda_3$, donc après identification : $\lambda_1+\lambda_2+\lambda_3 = -\dfrac{a_2}{a_3}$ (somme des racines), $\lambda_1\lambda_2\lambda_3 = -\dfrac{a_0}{a_3}$ (produit des racines) et $\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3 = \dfrac{a_1}{a_3}$.

Le résultat qui suit généralise les calculs précédents par simple développement du produit $\prod_{i=1}^{n}(X-\lambda_i)$.

Théorème **(Relations coefficients-racines)** Soit $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{C}[X]$ de degré $n \geqslant 1$ et de racines $\lambda_1, \dots, \lambda_n$ comptées avec multiplicité. Si on pose $\sigma_k = \sum_{1\leqslant i_1<\dots<i_k\leqslant n} \lambda_{i_1}\dots\lambda_{i_k}$ pour tout $k \in [\![1,n]\!]$, alors :

$$P = a_n\prod_{i=1}^{n}(X-\lambda_i) = a_n\Big(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} - \sigma_3X^{n-3} + \dots + (-1)^n\sigma_n\Big).$$

La relation obtenue ne nous permet pas d'exprimer les racines $\lambda_1, \dots, \lambda_n$ de P en fonction de ses coefficients $a_0, \dots, a_n$, mais nous pouvons en tirer $\sigma_1, \dots, \sigma_n$ en fonction de $a_0, \dots, a_n$ par identification. En l'occurrence : $\sigma_k = (-1)^k\dfrac{a_{n-k}}{a_n}$ pour tout $k \in [\![1,n]\!]$. Vues comme fonctions de $\lambda_1, \dots, \lambda_n$, les expressions $\sigma_1, \dots, \sigma_n$ sont appelées les *fonctions symétriques élémentaires de* $\lambda_1, \dots, \lambda_n$ — symétriques parce qu'elles ne dépendent pas de l'ordre dans lequel on a rangé $\lambda_1, \dots, \lambda_n$. Deux d'entre elles sont plus simples et plus utilisées que les autres :

$$\sigma_1 = \sum_{k=1}^{n}\lambda_k \quad \text{(somme des racines)} \qquad \text{et} \qquad \sigma_n = \prod_{k=1}^{n}\lambda_k \quad \text{(produit des racines)}.$$

Pour que tout soit bien clair, détaillons σ_1, σ_2, σ_3 et σ_4 dans le cas où $n = 4$: $\sigma_1 = \lambda_1+\lambda_2+\lambda_3+\lambda_4$, $\sigma_2 = \lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_1\lambda_4+\lambda_2\lambda_3+\lambda_2\lambda_4+\lambda_3\lambda_4$, $\sigma_3 = \lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_4+\lambda_1\lambda_3\lambda_4+\lambda_2\lambda_3\lambda_4$ et $\sigma_4 = \lambda_1\lambda_2\lambda_3\lambda_4$.

Exemple Pour tout $n \geqslant 2$: $\sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = \sum_{\omega\in\mathbb{U}_n}\omega = 0$ et $\prod_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = \prod_{\omega\in\mathbb{U}_n}\omega = (-1)^{n+1}$.

Démonstration Dans le contexte du polynôme scindé X^n-1 : $\sigma_1 = \sum_{\omega\in\mathbb{U}_n}\omega$ et $\sigma_n = \prod_{\omega\in\mathbb{U}_n}\omega$ et les relations coefficients-racines s'écrivent : $X^n - 1 = X^n - \sigma_1X^{n-1} + \dots + (-1)^n\sigma_n$, donc $\sigma_1 = 0$ et $\sigma_n = (-1)^{n+1}$.

Exemple Le polynôme non constant $X^3 - 2X + 5$ est scindé sur $\mathbb{C}$ d'après le théorème de d'Alembert-Gauss — mais pas forcément sur $\mathbb{R}$ — et nous pouvons noter x, y et z ses trois racines complexes comptées avec multiplicité. L'unique polynôme unitaire de degré 3 dont les racines sont x^2, y^2 et z^2 est alors le polynôme $X^3 - 4X^2 + 4X - 25$.
Remarquez bien qu'on arrive au résultat sans jamais avoir eu la moindre idée de ce que valent x, y et z !

Démonstration Nous devons calculer explicitement les coefficients du polynôme $\big(X-x^2\big)\big(X-y^2\big)\big(X-z^2\big)$:

$$\big(X-x^2\big)\big(X-y^2\big)\big(X-z^2\big) = X^3 - \big(x^2+y^2+z^2\big)X^2 + \big(x^2y^2+y^2z^2+z^2x^2\big)X - x^2y^2z^2.$$

Posons : $\sigma_1 = x+y+z$, $\sigma_2 = xy+yz+zx$ et $\sigma_3 = xyz$. Les relations coefficients-racines du polynôme $X^3 - 2X + 5$ s'écrivent : $\sigma_1 = 0$, $\sigma_2 = -2$ et $\sigma_3 = -5$. Or :

$$x^2+y^2+z^2 = (x+y+z)^2 - 2(xy+yz+zx) = \sigma_1^2 - 2\sigma_2 = 4, \qquad x^2y^2z^2 = (xyz)^2 = \sigma_3^2 = 25$$

et $x^2y^2+y^2z^2+z^2x^2 = (xy+yz+zx)^2 - 2\big(x^2yz+xy^2z+xyz^2\big) = \sigma_2^2 - 2xyz(x+y+z) = \sigma_2^2 - 2\sigma_1\sigma_3 = 4$.
Comme annoncé : $\big(X-x^2\big)\big(X-y^2\big)\big(X-z^2\big) = X^3 - 4X^2 + 4X - 25$.

4 Polynômes annulateurs d'une matrice carrée

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Pour tout $P = \sum_{k=0}^{+\infty} a_kX^k \in \mathbb{K}[X]$, on pose $P(A) = \sum_{k=0}^{+\infty} a_kA^k$. Le résultat de cette *évaluation en* A est une matrice carrée et non un polynôme, mais on dit que cette matrice carrée est un *polynôme en* A.

Attention ! Le polynôme constant 1 devient I_n quand on l'évalue en A. Par exemple, si $P = X^2+3$, alors $P(A) = A^2+3I_n$.

Définition-théorème **(Polynômes annulateurs d'une matrice carrée)** Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle *polynôme annulateur de A* tout polynôme $P \in \mathbb{K}[X]$ pour lequel $P(A) = 0$.

Attention ! On dit aussi que A *annule* P, mais jamais que A est « racine de P ». Les racines sont définitivement des éléments de $\mathbb{K}$.

Exemple Le polynôme $X^3 - 2X^2 - 1$ annule $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ car après calcul : $A^3 - 2A^2 - I_3 = 0$. Attention au terme I_3 !

Exemple Nous avons vu en TD que pour tout $A \in \mathcal{M}_2(\mathbb{C})$: $A^2 = \mathrm{tr}(A)A - \det(A)I_2$, donc le polynôme $X^2 - \mathrm{tr}(A)X + \det(A)$ annule A. Par exemple, $X^2 - 6X - 1$ annule $\begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$.

Théorème **(Deux remarques sur les polynômes annulateurs)** Soit $A \in \mathcal{M}_n(\mathbb{K})$.

(i) Si A possède un polynôme annulateur de degré d, tout polynôme en A est combinaison linéaire des puissances $I_n, A, A^2, \dots, A^{d-1}$.

(ii) Si A possède un polynôme annulateur dont le coefficient constant est non nul, alors A est inversible.

Démonstration Faisons l'hypothèse que A possède un polynôme annulateur $\Pi = a_d X^d + \dots + a_1 X + a_0$ avec $a_0, \dots, a_{d-1} \in \mathbb{C}$ et $a_d \in \mathbb{C}^*$.

(i) Soit $P \in \mathbb{C}[X]$. La division euclidienne de P par Π s'écrit $P = \Pi Q + R$ pour certains $Q, R \in \mathbb{C}[X]$ avec $\deg(R) < d$. Après évaluation en A : $P(A) = \Pi(A)Q(A) + R(A) = R(A)$, donc en effet, $P(A)$ est combinaison linéaire de $I_n, A, \dots, A^{d-1}$.

(ii) Supposons $a_0 \neq 0$. Par hypothèse : $-a_0 I_n = \sum_{k=1}^{n} a_k A^k = A \times \left(\sum_{k=1}^{n} a_k A^{k-1} \right) = \left(\sum_{k=1}^{n} a_k A^{k-1} \right) \times A$, donc A est inversible d'inverse $-\frac{1}{a_0} \sum_{k=1}^{n} a_k A^{k-1}$.

Exemple Reprenons la matrice $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ et son polynôme annulateur $X^3 - 2X^2 - 1$. Comme $A^3 - 2A^2 = I_3$, alors $A \times (A^2 - 2A) = (A^2 - 2A) \times A = I_3$, donc A est inversible et $A^{-1} = A^2 - 2A = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}$.

Les polynômes annulateurs d'une matrice carrée servent aussi à calculer ses puissances. Deux mots d'ordre en la matière, division euclidienne et racines !

Exemple On pose $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Pour tout $k \in \mathbb{N}^*$: $A^k = \frac{1}{3} \begin{pmatrix} 2^{k+1} + (-1)^k & 2^k - (-1)^k & 2^k - (-1)^k \\ 2^k - (-1)^k & 2^{k-1} + (-1)^k & 2^{k-1} + (-1)^k \\ 2^k - (-1)^k & 2^{k-1} + (-1)^k & 2^{k-1} + (-1)^k \end{pmatrix}$.

Démonstration $A^2 = \begin{pmatrix} 3 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ et $A^3 = \begin{pmatrix} 5 & 3 & 3 \\ 3 & 1 & 1 \\ 3 & 1 & 1 \end{pmatrix} = A^2 + 2A$, donc le polynôme $P = X^3 - X^2 - 2X$ annule A, et on peut l'écrire aussi $P = (X+1)X(X-2)$.

À présent, soit $k \in \mathbb{N}^*$. La division euclidienne de X^k par P s'écrit $X^k = PQ + aX^2 + bX + c$ avec $Q \in \mathbb{R}[X]$ et $a, b, c \in \mathbb{R}$. Évaluons en les racines de P : $(-1)^k = a - b + c$, $0 = c$ et $2^k = 4a + 2b + c$. Après calcul : $a = \frac{2^{k-1} + (-1)^k}{3}$, $b = \frac{2^{k-1} - 2(-1)^k}{3}$ et $c = 0$. Conclusion :

$$A^k = \underbrace{P(A)}_{=0} Q(A) + aA^2 + bA + cI_3 = \frac{2^{k-1} + (-1)^k}{3} \begin{pmatrix} 3 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} + \frac{2^{k-1} - 2(-1)^k}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

5 Polynômes d'interpolation de Lagrange

Étant donnés des points $x_1, \dots, x_n \in \mathbb{R}$ pour lesquels $x_1 < \dots < x_n$ et des réels $y_1, \dots, y_n \in \mathbb{R}$ quelconques, le problème de l'*interpolation* consiste à construire des fonctions $f : [x_1, x_n] \longrightarrow \mathbb{R}$ pour lesquelles $f(x_i) = y_i$ pour tout $i \in [\![1, n]\!]$. Il existe bien sûr beaucoup de telles fonctions f, on peut par exemple en construire une en reliant linéairement les points de coordonnées $(x_1, y_1), \dots, (x_n, y_n)$. La méthode d'*interpolation de Lagrange* étudiée dans ce paragraphe est une autre approche du même problème.

Définition **(Polynômes de Lagrange d'une famille de points distincts)** Soient $x_1,\dots,x_n \in \mathbb{K}$ DISTINCTS. Pour tout $i \in [\![1,n]\!]$, on pose $L_i = \prod_{\substack{1\leqslant k\leqslant n\\ k\neq i}} \frac{X-x_k}{x_i-x_k}$. Les polynômes $L_1,\dots,L_n$ sont appelés les *polynômes de Lagrange de* $x_1,\dots,x_n$.

Propriété fondamentale : Pour tous $i,j \in [\![1,n]\!]$: $L_i(x_j) = \delta_{ij}$.
En particulier, L_i admet $x_1,\dots,x_{i-1},x_{i+1},\dots,x_n$ pour racines — mais pas x_i.

Pour $n=3$: $L_1 = \frac{(X-x_2)(X-x_3)}{(x_1-x_2)(x_1-x_3)}$, $L_2 = \frac{(X-x_1)(X-x_3)}{(x_2-x_1)(x_2-x_3)}$ et $L_3 = \frac{(X-x_1)(X-x_2)}{(x_3-x_1)(x_3-x_2)}$.

Théorème **(Polynôme d'interpolation de Lagrange de degré minimal)** Soient $x_1,\dots,x_n \in \mathbb{K}$ DISTINCTS et $y_1,\dots,y_n \in \mathbb{K}$ quelconques. Avec les notations précédentes, $\sum_{i=1}^n y_i L_i$ est le seul polynôme $P \in \mathbb{K}[X]$ DE DEGRÉ STRICTEMENT INFÉRIEUR À n pour lequel $P(x_i) = y_i$ pour tout $i \in [\![1,n]\!]$.

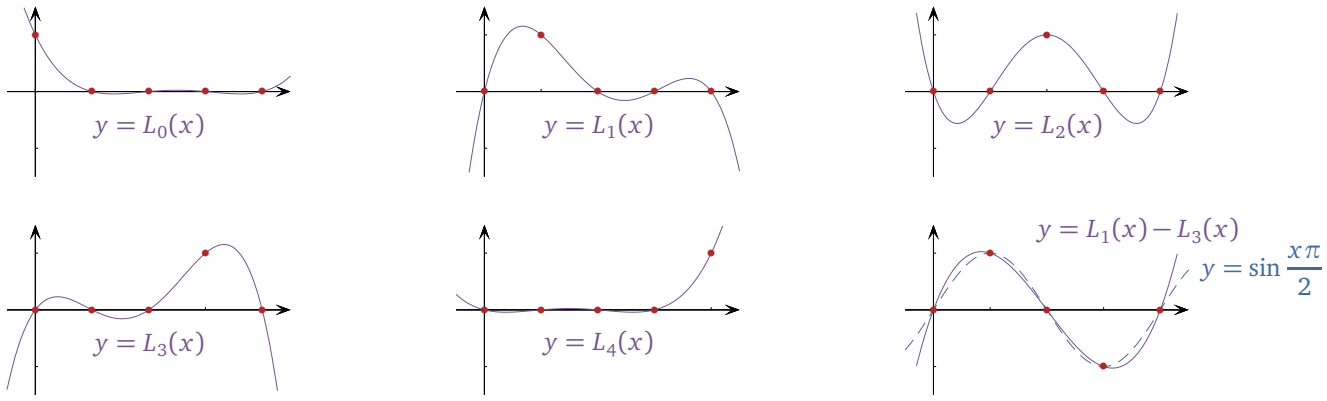
Démonstration

- **Existence :** Posons $P = \sum_{i=1}^n y_i L_i$. Par définition, $L_1,\dots,L_n$ sont de degrés au plus $n-1$, donc P aussi. Ensuite, pour tout $j \in [\![1,n]\!]$: $P(x_j) = \sum_{i=1}^n y_i L_i(x_j) = \sum_{i=1}^n y_i \delta_{ij} = y_j$.
- **Unicité :** Soient $P,Q \in \mathbb{K}[X]$ deux polynômes de degrés au plus $n-1$ pour lesquels $P(x_i) = Q(x_i) = y_i$ pour tout $i \in [\![1,n]\!]$. Le polynôme $P-Q$ admet $x_1,\dots,x_n$ pour racines, donc au moins n racines comptées avec multiplicité. Comme $\deg(P-Q) \leqslant n-1$, forcément $P-Q=0$, i.e. $P=Q$.

Exemple Notons f la fonction $x \longmapsto \sin\frac{x\pi}{2}$ sur $[0,4]$, pour laquelle : $f(0) = f(2) = f(4) = 0$, $f(1) = 1$ et $f(3) = -1$. Notons ensuite $L_0,\dots,L_4$ les cinq polynômes de Lagrange de $0,\dots,4$. Le polynôme d'interpolation de Lagrange de f aux points $0,\dots,4$ est alors en vertu du théorème précédent le polynôme $\sum_{i=0}^4 f(i)L_i = L_1 - L_3$. Or :

$$L_1 = -\frac{X(X-2)(X-3)(X-4)}{6} \quad \text{et} \quad L_3 = -\frac{X(X-1)(X-2)(X-4)}{6},$$

donc : $L_1 - L_3 = -\frac{X(X-2)(X-3)(X-4)}{6} + \frac{X(X-1)(X-2)(X-4)}{6} = \frac{X(X-2)(X-4)}{3}$.



Théorème **(Polynômes d'interpolation de Lagrange, cas général)** On reprend les notations précédentes et on note Y le polynôme $\sum_{i=1}^n y_i L_i$. Les polynômes P pour lesquels $P(x_i) = y_i$ pour tout $i \in [\![1,n]\!]$ sont exactement tous les polynômes de la forme $Y + Q\prod_{k=1}^n (X-x_k)$, Q décrivant $\mathbb{K}[X]$.

Démonstration Pour tout $P \in \mathbb{K}[X]$:
$$\forall i \in [\![1,n]\!],\ P(x_i) = y_i \iff \forall i \in [\![1,n]\!],\ P(x_i) = Y(x_i)$$
$$\iff P - Y \text{ admet } x_1,\dots,x_n \text{ pour racines} \iff \prod_{k=1}^n (X-x_k) \text{ divise } P-Y$$
$$\iff \exists Q \in \mathbb{K}[X],\ P - Y = Q\prod_{k=1}^n (X-x_k).$$

6 Preuve du théorème de d'Alembert-Gauss

Nous terminerons ce chapitre sur une preuve — hors programme — du théorème de d'Alembert-Gauss. Mais d'abord un lemme technique intéressant en soi.

Théorème **(On peut toujours tomber plus bas)** Soient $Q \in \mathbb{C}[X]$ non constant et $a \in \mathbb{C}$. Si $Q(a) \neq 0$, alors $\big|Q(z)\big| < \big|Q(a)\big|$ pour un certain $z \in \mathbb{C}$.

Démonstration Quitte à remplacer Q par $\dfrac{Q(X+a)}{Q(a)}$, on peut supposer sans perte de généralité que $a = 0$ et $Q(0) = 1$. Notons alors d le degré de Q — Q est non constant, donc $d \geqslant 1$ — et écrivons Q sous la forme $Q = 1 + b_q X^q + b_{q+1}X^{q+1} + \ldots + b_d X^d$ où b_q est le premier coefficient non nul de Q autre que son coefficient constant. Notons enfin β_q une racine $q^{\text{ème}}$ de $-\dfrac{1}{b_q}$. Quitte à remplacer Q par $Q(\beta_q X)$, on peut supposer de nouveau sans perte de généralité que $b_q = -1$, de sorte que $Q = 1 - X^q + b_{q+1}X^{q+1} + \ldots + b_d X^d$. Finalement, pour tout $r \in [0,1]$: $\big|Q(r)\big| = \big|1 - r^q + \ldots + b_d r^d\big| \leqslant \big|1-r^q\big| + \displaystyle\sum_{k=q+1}^{d} |b_k| r^k \overset{r\in[0,1]}{\leqslant} 1 - r^q + r^{q+1}\sum_{k=q+1}^{d}|b_k| = 1 - (1 - Mr)r^q$ si on pose $M = \displaystyle\sum_{k=q+1}^{d}|b_k|$. Comme voulu, $\big|Q(r)\big| < 1$ si on choisit r assez petit.

Et maintenant, le théorème de d'Alembert-Gauss.

Démonstration **(du théorème de d'Alembert-Gauss)** Soit $P \in \mathbb{C}[X]$ non constant. Pour montrer que P possède une racine dans $\mathbb{C}$, nous allons nous intéresser à la fonction $|P|$, prouver qu'elle possède un minimum et que celui-ci vaut 0. Cela garantira bien l'existence d'une racine. Il nous suffit d'ailleurs de justifier l'existence du minimum, car une fois qu'il existe, le minimum ne peut qu'être nul d'après le lemme, sans quoi on pourrait tomber plus bas.

Introduisons les coefficients de P : $P = a_d X^d + \ldots + a_1 X + a_0$ avec $d = \deg(P) \geqslant 1$, $a_0, \ldots, a_{d-1} \in \mathbb{C}$ et $a_d \in \mathbb{C}^*$. Positive, la fonction $|P|$ possède une borne inférieure $m = \inf_{\mathbb{C}} |P|$ d'après la propriété de la borne inférieure, mais s'agit-il d'un minimum ?

- Pour tous $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$ de module n :
$$\big|P(z)\big| \geqslant \big|a_d z^d\big| - \left|\sum_{k=0}^{d-1} a_k z^k\right| \geqslant |a_d| n^d - \sum_{k=0}^{d-1}|a_k| n^k \xrightarrow[n\to+\infty]{} +\infty,$$
donc $|a_d| n^d - \displaystyle\sum_{k=0}^{d-1}|a_k| n^k > m+1$ à partir d'un certain rang N. Ainsi, pour tout $z \in \mathbb{C}$:
$$|z| > N \quad\Longrightarrow\quad \big|P(z)\big| > m+1.$$
- À présent, pour tout $n \in \mathbb{N}$, $m + \dfrac{1}{2^n}$ ne minore pas $|P|$, donc $\big|P(z_n)\big| < m + \dfrac{1}{2^n}$ pour un certain $z_n \in \mathbb{C}$ — et même $m \leqslant \big|P(z_n)\big| < m + \dfrac{1}{2^n}$. Par encadrement : $\lim\limits_{n\to+\infty} \big|P(z_n)\big| = m$.
- Finalement, pour tout $n \in \mathbb{N}$: $\big|P(z_n)\big| < m + \dfrac{1}{2^n} \leqslant m+1$, donc $|z_n| \leqslant N$ d'après le premier point. Bornée, la suite $(z_n)_{n\in\mathbb{N}}$ possède une suite extraite convergente $\big(z_{\varphi(n)}\big)_{n\in\mathbb{N}}$ d'après le théorème de Bolzano-Weierstrass. En notant ℓ sa limite : $m = \lim\limits_{n\to+\infty} \big|P\big(z_{\varphi(n)}\big)\big| = \big|P(\ell)\big|$, donc m est le minimum de $|P|$ et pas seulement sa borne inférieure.