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 ici.

1 Construction de l'anneau $\mathbb{K}[X]$ des polynômes

Vous n'avez pas distingué jusqu'ici les « polynômes » des « fonctions polynomiales ». Ce sont pour vous toutes les fonctions définies sur $\mathbb{R}$ de la forme $x \longmapsto a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ pour certains $n \in \mathbb{N}$ et $a_0, a_1, \ldots, a_n \in \mathbb{R}$. Nous allons dans ce chapitre apprendre à distinguer soigneusement les deux concepts : non, les « polynômes » ne sont pas des fonctions.

Imaginez un anneau A dans lequel vous avez le droit de multiplier chaque objet par un réel. Vous savez donc faire trois choses : additionner et multiplier les éléments de A entre eux et multiplier chacun par un réel. Dans un tel univers, vous pouvez parler de polynômes. Pour tout $a \in A$, la quantité $3a^2 + 4a + 1_A$ est bien définie et on a bien envie de la noter $P(a)$, où $P = 3X^2 + 4X + 1$.

Pourquoi hélas cet exemple ruine-t-il la possibilité qu'on conçoive les polynômes comme des fonctions ? Si le polynôme P était une fonction, ce serait la fonction $x \longmapsto 3x^2 + 4x + 1$ définie sur $\mathbb{R}$, éventuellement sur $\mathbb{C}$. Or dans notre exemple, a n'est pas un nombre a priori car nous savons seulement de A que c'est un anneau dans lequel on sait multiplier par un réel. Bizarrement, $P(a)$ n'est pas « la fonction P évaluée en a » puisque a n'a pas de raison d'appartenir au domaine de définition de P — $P(a)$ est une simple **notation** pour l'élément abstrait $3a^2 + 4a + 1_A$ de A.

Une question d'importance se pose alors : les univers A existent-ils réellement ? La réponse est oui, nous en connaissons même un certain nombre : l'ensemble $\mathbb{R}$ tout d'abord, mais aussi l'ensemble $\mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, et enfin l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites réelles. Mais d'autres univers de ce genre nous attendent. Nous saurons bientôt additionner, multiplier et multiplier par un réel ce qu'on appelle les *matrices*, qui sont des tableaux de nombres comme $\begin{pmatrix} 7 & 3 \\ 2 & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 3 & 0 \\ -6 & 2 & 5 \\ 3 & 1 & 1 \end{pmatrix}$. Pour diverses raisons, la notion de *polynôme de matrice* nous sera alors essentielle.

Dans chacun de ces univers, qu'est-ce qui importe au fond à la notion de polynôme ? L'essentiel du polynôme $3X^2 + 4X + 1$ n'est pas la nature de son indéterminée X, qu'on a pu tour à tour voir comme un nombre, une fonction, une suite, voire une matrice. Ce qui compte, ce sont ses coefficients et l'ordre dans lequel ils sont rangés, disons $(1, 4, 3)$ — degré 0, degré 1, degré 2. Vous voilà prêts enfin pour la définition suivante :

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 une indéterminée 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 allons bientôt pouvoir **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. Je vous conseille néanmoins d'avoir d'ores et déjà cette notation en tête si vous voulez bien 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 de $\mathbb{K}[X]$ sont égaux si et seulement si leurs coefficients sont égaux. Bref, les polynômes $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont égaux si et seulement si $a_k = b_k$ pour tout $k \in \mathbb{N}$.

Définition (Polynôme constant, polynôme nul) On appelle *polynôme constant* (*de* $\mathbb{K}[X]$) tout polynôme de $\mathbb{K}[X]$ de la forme $(\lambda, 0, 0, \ldots)$ pour un certain $\lambda \in \mathbb{K}$. Un tel polynôme est alors simplement noté λ.

Avec cette notation, le polynôme 0 est appelé le *polynôme nul* (*de* $\mathbb{K}[X]$).

Définition (Degré d'un polynôme, coefficient dominant, polynôme unitaire) Soit $P=(a_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$ **non nul**. Le plus grand indice k pour lequel $a_k\neq 0$ est appelé le *degré de* P et noté $\partial^\circ P$. Le coefficient de degré $\partial^\circ P$ 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 $-\infty$: $\quad\partial^\circ 0=-\infty$.

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

Tâchons maintenant de définir propement l'addition et la multiplication sur $\mathbb{K}[X]$ que notre intuiton appelle de ses vœux. Si $P=\sum_{k=0}^{n}a_kX^k$ et $Q=\sum_{k=0}^{n}b_kX^k$ sont des polynômes au sens intuitif du terme — comme les coefficients de P et Q sont nuls à partir d'un certain rang n, on peut prendre le même n pour P **et** Q — voici le genre de calculs qu'on a bien envie de faire :

$$P+Q=\sum_{k=0}^{n}a_kX^k+\sum_{k=0}^{n}b_kX^k=\sum_{k=0}^{n}(a_k+b_k)X^k$$

$$\text{et}\quad PQ=\sum_{i=0}^{n}a_iX^i\times\sum_{j=0}^{n}b_jX^j=\sum_{0\leqslant i,j\leqslant n}a_ib_jX^{i+j}=\sum_{k=0}^{2n}\sum_{\substack{0\leqslant i,j\leqslant n\\ i+j=k}}a_ib_jX^k=\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}a_lb_{k-l}\right)X^k.$$

On a ici regroupé les termes en fonction de leur degré. La définition suivante devrait maintenant vous paraître naturelle.

Définition (Anneau $\mathbb{K}[X]$) On définit ici deux lois $+$ et $\times$ de composition internes sur $\mathbb{K}[X]$. Soient $P,Q\in\mathbb{K}[X]$, $P=(a_k)_{k\in\mathbb{N}}$ et $Q=(b_k)_{k\in\mathbb{N}}$.

- On appelle *somme de P et Q* le polynôme $\big(a_k+b_k\big)_{k\in\mathbb{N}}$, noté $P+Q$.
- On appelle *produit de P et Q* le polynôme $\left(\sum_{i=0}^{k}a_ib_{k-i}\right)_{k\in\mathbb{N}}$, noté $P\times Q$ ou PQ.
  En particulier, pour tout $\lambda\in\mathbb{K}$, λP est le polynôme $(\lambda a_k)_{k\in\mathbb{N}}$.

Alors $\big(\mathbb{K}[X],+,\times\big)$ est un anneau commutatif. Elément neutre pour $+$: le polynôme nul 0 ; et pour $\times$: le polynôme 1.

✖✖✖ **Attention !** Pour le moment, nous n'avons pas de fractions rationnelles à notre disposition. Les écritures de la forme $\dfrac{X^2+1}{X+2}$ sont bannies jusqu'à nouvel ordre. Nous les retrouverons en fin d'année.

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

- Vérifions tout d'abord que la somme et le produit de deux polynômes sont bien des polynômes — pour garantir qu'on a bien des lois de composition internes. Notons N un rang à partir duquel $a_k=b_k=0$.

  1) D'abord $P+Q$ est un polynôme car ses coefficients a_k+b_k sont nuls à partir du rang N.

  2) Ensuite, soit $k\geqslant 2N$. Pour tout $i\in[\![0,k]\!]$, l'un des entiers i et $k-i$ est supérieur ou égal à N, car si $i<N$, alors $k-i>k-N\geqslant 2N-N=N$. En particulier $a_i=0$ ou $b_{k-i}=0$, donc $a_ib_{k-i}=0$, puis par somme $\sum_{i=0}^{k}a_ib_{k-i}=0$. Les coefficients de PQ sont nuls à partir du rang $2N$ donc PQ est un polynôme.

- Soit $\lambda\in\mathbb{K}$. A quoi le polynôme λP ressemble-t-il ? Pour tout $k\in\mathbb{N}$, le coefficient de degré k de λP vaut : $\lambda a_k+0.a_{k-1}+0.a_{k-2}+\ldots+0.a_0=\lambda a_k$, donc $\lambda P=(\lambda a_k)_{k\in\mathbb{N}}$.

- L'associativité et la commutativité de $+$ sont évidentes. En outre le polynôme nul est élément neutre pour $+$ et l'inverse pour $+$ de $P=(a_k)_{k\in\mathbb{N}}$ est $-P=(-a_k)_{k\in\mathbb{N}}$. Conclusion : $\big(\mathbb{K}[X],+\big)$ est un groupe commutatif.

- Montrons la commutativité de $\times$. Pour tout $k\in\mathbb{N}$: $\sum_{i=0}^{k}a_ib_{k-i}=\sum_{j=0}^{k}b_ja_{k-j}$ après le changement d'indice $i+j=k$. Bref : PQ et QP ont les mêmes coefficients donc sont égaux.

- Le polynôme constant 1 est élément neutre pour $\times$.

- Montrons l'associativité de $\times$. Pour tout $k\in\mathbb{N}$, le coefficient de degré k de $(PQ)R$ est :

$$\sum_{i=0}^{k}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)c_{k-i}=\sum_{0\leqslant j\leqslant i\leqslant k}a_jb_{i-j}c_{k-i}=\sum_{j=0}^{k}a_j\left(\sum_{i=j}^{k}b_{i-j}c_{k-i}\right)\overset{l=i-j}{=}\sum_{j=0}^{k}a_j\left(\sum_{l=0}^{k-j}b_lc_{(k-j)-l}\right).$$

  Le terme obtenu se trouve être égal au coefficient de degré k de $P(QR)$. Par conséquent $(PQ)R$ et $P(QR)$ ont les mêmes coefficients, donc sont égaux.

- Montrons que $\times$ est distributive sur $+$. Pour tout $k \in \mathbb{N}$, le coefficient de degré k de $P(Q+R)$ est :

$$\sum_{i=0}^{k} a_i(b_{k-i} + c_{k-i}) = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i}.$$

Le terme obtenu se trouve être égal au coefficient de degré k de $(PQ)+(PR)$. Par conséquent $P(Q+R)$ et $(PQ)+(PR)$ ont les mêmes coefficients, sont donc égaux. ■

Et voilà, le temps de la notation polynomiale des polynômes est enfin venu ! Désormais, grâce au théorème suivant, les polynômes seront notés comme des polynômes au sens intuitif du terme. Je ne vous conseille certainement pas d'oublier la construction que nous venons d'effectuer, mais il est vrai tout de même que nous ne verrons plus jamais les polynômes apparaître sous forme de suites dans ce cours.

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

- Pour tout $k \in \mathbb{N}$, X^k est le polynôme $(0,\ldots,0,1,0,0,\ldots)$ dans lequel le coefficient 1 est placé en $(k+1)^{\text{ème}}$ position :

$$1 = (1,0,0,\ldots), \qquad X = (0,1,0,0,\ldots), \qquad X^2 = (0,0,1,0,0,\ldots), \qquad X^3 = (0,0,0,1,0,0,\ldots)\ldots$$

- Pour tout polynôme non nul $P = (a_k)_{k\in\mathbb{N}}$ de degré n, $P = \sum_{k=0}^{n} a_k X^k$.

Pour tout $k \in [\![0,n]\!]$, le polynôme $a_k X^k$ est appelé le *monôme de degré k de P*.

- Tout polynôme peut être écrit d'une unique façon sous la forme d'une somme $\sum_{k=0}^{\infty} a_k X^k$ où $(a_k)_{k\in\mathbb{N}}$ est une suite d'éléments de $\mathbb{K}$. Une telle somme, contrairement aux apparences, est **finie** par définition des polynômes. La notation « somme infinie » rend cependant de précieux services de rédaction.

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

Définition (Composition des polynômes)

- Soient $P = \sum_{k=0}^{\infty} a_k X^k, Q \in \mathbb{K}[X]$. On appelle *composée de Q suivie de P*, noté $P \circ Q$, le polynôme $P \circ Q = \sum_{k=0}^{\infty} a_k Q^k$.
- La composition $\circ$ est associative et distributive **à droite** par rapport à l'addition $+$ et à la multiplication $\times$. Pour tous $P, Q, R \in \mathbb{K}[X]$:

$$(P\circ Q)\circ R = P\circ(Q\circ R), \qquad (PQ)\circ R = (P\circ R)\times(Q\circ R) \qquad \text{et} \qquad (P+Q)\circ R = (P\circ R)+(Q\circ R).$$

Démonstration Débrouillez-vous. ■

✖✖✖ **Attention !** La composition n'est pas distributive à gauche par rapport à l'addition et à la multiplication.

$$\begin{cases} X^2\circ(X+1) = (X+1)^2 \\ (X^2\circ X)+(X^2\circ 1) = X^2+1 \end{cases} \quad \text{(addition)} \qquad \text{et} \qquad \begin{cases} (X+1)\circ(X\times X) = X^2+1 \\ \big((X+1)\circ X\big)\times\big((X+1)\circ X\big) = (X+1)^2 \end{cases} \quad \text{(multiplication).}$$

Théorème (Opérations sur les polynômes et degré) Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

(i) **Degré d'une somme :** $\partial^\circ(P+Q) \leqslant \max\left\{\partial^\circ P, \partial^\circ Q\right\}$.
Cette inégalité est stricte si et seulement si P et Q ont le même degré et des coefficients dominants opposés.

(ii) **Degré d'un produit :** $\partial^\circ(PQ) = \partial^\circ P + \partial^\circ Q$.
En particulier, si $\lambda \neq 0$, $\partial^\circ(\lambda P) = \partial^\circ P$.

(iii) **Degré d'une composée :** Si Q n'est pas constant : $\partial^\circ(P\circ Q) = \partial^\circ P \times \partial^\circ Q$.

Démonstration Toutes les formules du théorème sont évidentes dans le cas où $P=0$ ou $Q=0$. Supposons donc P et Q non nuls et notons $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$, m le degré de P et n celui de Q.

(i) Clairement, quand on calcule la somme de P et Q, les coefficients de degré strictement supérieur au maximum des degrés de P et Q sont nuls. D'où l'inégalité $\partial^\circ(P+Q) \leqslant \max\left\{\partial^\circ P, \partial^\circ Q\right\}$.

(ii) Montrons que $\partial^\circ(PQ) = m+n$. Pour tout $k \in \mathbb{N}$, notons $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ le coefficient de degré k de PQ.

1) Montrons d'abord que $c_{m+n} = a_m b_n$ — comme $a_m b_n \neq 0$, cela montrera que $\partial^\circ(PQ) \geqslant m+n$. Dans la somme définissant c_{m+n}, si $i < m$, alors $(m+n) - i > (m+n) - m = n$ donc $b_{m+n-i} = 0$; et si $i > m$, alors $a_i = 0$. Seul le terme d'indice $i = m$ peut être non nul, donc enfin $c_{m+n} = a_m b_n$.

2) Ensuite, soit $k \geqslant m+n+1$. Montrons que $c_k = 0$ — cela montrera que $\partial^\circ(PQ) \leqslant m+n$. Dans la somme définissant c_k, si $i \leqslant m$, alors $k - i \geqslant k - m \geqslant (m+n+1) - m = n+1$, et donc $b_{k-i} = 0$; et si $i > m$, alors $a_i = 0$. Tous les termes de la somme étant nuls, on obtient bien $c_k = 0$.

(iii) Montrons que si Q est non constant, i.e. si $\partial^\circ Q \geqslant 1$, alors $\partial^\circ(P \circ Q) = \partial^\circ P \times \partial^\circ Q$.
Pour tout $k \in [\![0, m]\!]$, $\partial^\circ(Q^k) = k\partial^\circ Q$ d'après (ii). Or comme $\partial^\circ Q \geqslant 1$, la suite $\left(\partial^\circ Q^k\right)_{0 \leqslant k \leqslant m}$ est strictement croissante. Du coup, d'après (i) : $\partial^\circ(P \circ Q) = \partial^\circ\left(\sum_{k=0}^{m} a_k Q^k\right) \overset{a_m \neq 0}{=} \partial^\circ Q^m = m\partial^\circ Q = mn$. ■

Théorème (Intégrité de $\mathbb{K}[X]$) $\mathbb{K}[X]$ est intègre, i.e. : $\forall P, Q \in \mathbb{K}[X], \quad \Big(PQ = 0 \implies P = 0 \text{ ou } Q = 0\Big)$.

✌ ✌ ✌ **Explication** Remercions les mathématiciens d'avoir inventé les polynômes et rejeté en partie les fonctions polynomiales. Si on travaillait ici avec des fonctions polynomiales et non avec des polynômes, ce théorème serait nettement plus difficile à démontrer. En effet, si on a $P(x)Q(x) = 0$ 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.

Démonstration Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $\partial^\circ(PQ) = -\infty$. Or $\partial^\circ(PQ) = \partial^\circ P + \partial^\circ Q$, donc nécessairement $\partial^\circ P = -\infty$ ou $\partial^\circ Q = -\infty$, i.e. $P = 0$ ou $Q = 0$. ■

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

• Le polynôme $\sum_{k=0}^{\infty} k a_k X^{k-1}$ est appelé le *polynôme dérivé de P* et noté P' (par convention $0 \times X^{-1} = 0$, c'est pourquoi dans cette définition X^{-1} apparaît faussement).

• On définit alors par récurrence la suite des polynômes dérivés de P. Pour commencer, le $0^{ème}$ *polynôme dérivé de P* est $P^{(0)} = P$. Ensuite, pour tout $n \in \mathbb{N}$, le $(n+1)^{ème}$ *polynôme dérivé de P*, noté $P^{(n+1)}$, est le polynôme dérivé du $n^{\text{ème}}$ polynôme dérivé de P : $P^{(n+1)} = \left(P^{(n)}\right)'$.
Pour $n = 1$ et $n = 2$ respectivement, on note plutôt P' et P'' que $P^{(1)}$ et $P^{(2)}$.

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

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

(i) **Degré :** $\partial^\circ P^{(n)} = \partial^\circ P - n$ si $n \leqslant \partial^\circ P$, et $P^{(n)} = 0$ sinon.

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

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

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

✖ ✖ ✖ **Attention !** La formule de Leibniz ressemble certes à la formule du binôme de Newton et elle se démontre de la même façon, mais elle fait apparaître les **dérivées** de P et Q et non leurs puissances.

Démonstration Introduisons $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ la suite des coefficients de P et Q respectivement.

(i) Nous pouvons supposer P non nul et noter d son degré, de sorte que $a_d \neq 0$. Si $d = 0$, $P' = 0$ comme le veut le théorème. Si au contraire $d \geqslant 1$, alors par définition $P' = \sum_{k=0}^{d} k a_k X^{k-1}$ avec $d a_d \neq 0$, donc $\partial^\circ P' = d - 1$.
On généralise par récurrence aux cas des dérivées successives.

(iii) Commençons par démontrer la formule « $(PQ)' = P'Q + PQ'$ ».

$$(PQ)' = \left[\sum_{k=0}^{\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^k\right]' = \sum_{k=1}^{\infty} k\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^{k-1} = \sum_{k=1}^{\infty}\left(\sum_{i=0}^{k} k a_i b_{k-i}\right)X^{k-1} \overset{l=k-1}{=} \sum_{l=0}^{\infty}\left(\sum_{i=0}^{l+1}(l+1)a_i b_{l+1-i}\right)X^l$$
$$= \sum_{l=0}^{\infty}\left(\sum_{i=0}^{l+1} i a_i b_{l+1-i} + \sum_{i=0}^{l+1} a_i(l+1-i)b_{l+1-i}\right)X^l = \sum_{l=0}^{\infty}\left(\sum_{i=1}^{l+1} i a_i b_{l+1-i}\right)X^l + \sum_{l=0}^{\infty}\left(\sum_{i=0}^{l} a_i(l+1-i)b_{l+1-i}\right)X^l$$
$$\overset{j=i-1}{=} \sum_{l=0}^{\infty}\left(\sum_{j=0}^{l}(j+1)a_{j+1}b_{l-j}\right)X^l + \sum_{l=0}^{\infty}\left(\sum_{i=0}^{l} a_i(l+1-i)b_{l+1-i}\right)X^l = P'Q + PQ'.$$

Déduisons-en par récurrence sur n la formule de Leibniz. **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 $P, Q \in \mathbb{K}[X]$.

$$(PQ)^{(n+1)} = \big((PQ)'\big)^{(n)} = (P'Q + PQ')^{(n)} \overset{\text{(ii)}}{=} (P'Q)^{(n)} + (PQ')^{(n)} = \sum_{k=0}^{n}\binom{n}{k}(P')^{(k)}Q^{(n-k)} + \sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}(Q')^{(n-k')}$$
$$= \sum_{k=0}^{n}\binom{n}{k}P^{(k+1)}Q^{(n-k)} + \sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}Q^{(n+1-k')} \overset{l=k+1}{=} \sum_{l=1}^{n+1}\binom{n}{l-1}P^{(l)}Q^{(n+1-l)} + \sum_{k'=0}^{n}\binom{n}{k'}P^{(k')}Q^{(n+1-k')}$$
$$= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\binom{n}{k-1}P^{(k)}Q^{(n+1-k)} + \sum_{k=1}^{n}\binom{n}{k}P^{(k)}Q^{(n+1-k)} + P^{(0)}Q^{(n+1)}$$
$$= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]P^{(k)}Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} \qquad \text{Utilisons la formule de Pascal.}$$
$$= P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)} + P^{(0)}Q^{(n+1)} = \sum_{k=0}^{n+1}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)}.$$

(iv) Par définition $P\circ Q = \sum_{k=0}^{\infty} a_k Q^k$, donc $(P\circ Q)' = \sum_{k=0}^{\infty} a_k\big(Q^k\big)'$. Or il n'est pas dur de montrer par récurrence à partir de la formule de dérivation d'un produit que $\big(Q^k\big)' = kQ'Q^{k-1}$ pour tout $k \in \mathbb{N}$, avec la convention que $0 \times Q^{-1} = 0$. Comme voulu : $(P\circ Q)' = \sum_{k=0}^{\infty} a_k \times kQ'Q^{k-1} = Q' \times P'\circ Q$. ■

2 Division dans $\mathbb{K}[X]$

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 $P \in \mathbb{K}[X]$ tel que $B = AP$. Cette relation se note $A|B$.

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

✌ ✌ ✌ **Explication** La relation de divisibilité peut être introduite dans tout anneau en réalité ($\mathbb{Z}$, $\mathbb{K}[X]$, $\mathbb{Z}[i]\dots$). Elle est en un sens ce qui différencie les anneaux les uns des autres et le point de départ de ce qu'on appelle en général l'*arithmétique*. L'arithmétique ne concerne pas seulement les entiers, elle a un sens bien au-delà comme théorie de la divisibilité dans les anneaux.

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

(i) La relation de divisibilité | sur $\mathbb{K}[X]$ est réflexive et transitive. Elle n'est cependant pas antisymétrique puisque :

$$A|B \quad \text{et} \quad B|A \qquad \Longleftrightarrow \qquad \exists\, \lambda \in \mathbb{K}^* / \quad A = \lambda B.$$

On dit alors que A et B sont *associés* (*sur* $\mathbb{K}$).

(ii) **Combinaisons linéaires :** Si $D|A$ et si $D|B$, alors $D|(\lambda A + \mu B)$ pour tous $\lambda, \mu \in \mathbb{K}$.

(iii) **Produit :** Si $A|B$ et si $C|D$, alors $AC|BD$. En particulier, si $A|B$, alors $A^k|B^k$ pour tout $k \in \mathbb{N}$.

(iv) **Multiplication/division par un polynôme :** Si $D \neq 0$: $\quad A|B \quad \Longleftrightarrow \quad AD|BD$.

Démonstration

(i) Pour le défaut d'antisymétrie, l'une des deux implications est triviale : si $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$, i.e. $B = \dfrac{1}{\lambda} A$, alors $A|B$ et $B|A$. Réciproquement, supposons que $A|B$ et $B|A$. Il existe alors $P, Q \in \mathbb{K}[X]$ tels que $A = BQ$ et $B = AP$, donc $A = APQ$. Deux cas se présentent alors.

- Si $A = 0$, alors $B = AP = 0$, et donc en posant $\lambda = 1$ on a bien $A = \lambda B$.
- Si au contraire $A \neq 0$, $PQ = 1$ par intégrité de $\mathbb{K}[X]$. En particulier P et Q sont non nuls, donc de degrés entiers. Finalement, les inégalités $0 \leqslant \partial^\circ P \leqslant \partial^\circ P + \partial^\circ Q = \partial^\circ(PQ) = \partial^\circ 1 = 0$ montrent que $\partial^\circ P = 0$, i.e. que P est un polynôme constant non nul. Notons-le λ. On a comme voulu $A = \lambda B$ et $\lambda \in \mathbb{K}^*$.

(iv) Supposons $D \neq 0$. Si $A|B$, alors $AD|BD$ d'après (iii). Réciproquement, si $AD|BD$, $BD = APD$ pour un certain $P \in \mathbb{K}[X]$. Or $\mathbb{K}[X]$ est intègre et $D \neq 0$, donc $B = AP$. Ceci montre bien que $A|B$. ■

2.2 Division euclidienne

Le théorème suivant montre que les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ se ressemblent énormément du point de vue de l'arithmétique, c'est-à-dire de la divisibilité. La suite du chapitre approfondira peu à peu cette remarque.

Théorème (Division euclidienne dans $\mathbb{K}[X]$) Soient $A, B \in \mathbb{K}[X]$, $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que $A = BQ + R$ et $\partial^\circ R < \partial^\circ B$.

Dans cet énoncé, A est appelé le *dividende*, B le *diviseur*, Q le *quotient* et R le *reste*.

Démonstration

- **Existence du couple (Q, R) :** Soient $b \in \mathbb{N}$ le degré de B et $\beta \neq 0$ son coefficient dominant.
  Si B divise A, $A = BQ$ pour un certain $Q \in \mathbb{K}[X]$ et on peut poser $R = 0$. Supposons désormais que B ne divise pas A. L'ensemble $\mathcal{D} = \left\{\partial^\circ(A - BK)\right\}_{K \in \mathbb{K}[X]}$ est alors une partie non vide de $\mathbb{N}$ — valeur $-\infty$ exclue par hypothèse — donc possède un plus petit élément $r \in \mathbb{N}$. Introduisons $Q \in \mathbb{K}[X]$ un polynôme pour lequel $\partial^\circ(A - BQ) = r$, posons $R = A - BQ$ et notons ρ le coefficient dominant de R. Il nous reste à prouver que $\partial^\circ R < \partial^\circ B$, i.e. que $r < b$.
  Raisonnons par l'absurde en supposant $r \geqslant b$. Alors $\partial^\circ\left(R - \dfrac{\rho}{\beta} X^{r-b} B\right) < r$ puisque la soustraction par $\dfrac{\rho}{\beta} X^{r-b} B$ tue le terme dominant ρX^r de R. Or $\partial^\circ\left(R - \dfrac{\rho}{\beta} X^{r-b} B\right) = \partial^\circ(A - BK) \in \mathcal{D}$ si l'on pose $K = Q + \dfrac{\rho}{\beta} X^{r-b}$. La minimalité de r est ainsi contredite. Comme voulu, $r < b$.
- **Unicité du couple (Q, R) :** Soient (Q_1, R_1) et (Q_2, R_2) deux couples associés à la division euclidienne de A par B. Alors $A = BQ_1 + R_1 = BQ_2 + R_2$, donc $B(Q_1 - Q_2) = R_2 - R_1$.
  Supposons $Q_1 \neq Q_2$. Alors $\partial^\circ(Q_1 - Q_2) \geqslant 0$, et donc $\partial^\circ B(Q_1 - Q_2) \geqslant \partial^\circ B$. Or $\partial^\circ(R_2 - R_1) < \partial^\circ B$ par définition de R_1 et R_2. Contradiction. Conclusion : $Q_1 = Q_2$, puis $R_1 = A - BQ_1 = A - BQ_2 = R_2$. ■

✎ ✎ ✎ **En pratique (Algorithme de la division euclidienne)** Comme dans $\mathbb{Z}$, la démonstration précédente nous fournit un algorithme facilement utilisable. Illustrons par exemple la division euclidienne de $7X^5 + 4X^4 + 2X^3 - X + 5$ par $X^2 + 2$.

Laisser la place des monômes de degré 2
même s'il n'en apparaît pas pour le moment.

$$\begin{array}{rl|l} 7X^5 + 4X^4 + 2X^3 \times - X + 5 & X^2 + 2 \\ \hline -7X^5 \quad -14X^3 & 7X^3 \\ \hline 4X^4 - 12X^3 - X + 5 & \end{array}$$

On divise $7X^5$ par X^2. Résultat : $7X^3$.
On retranche ensuite $7X^3(X^2 + 2)$ du polynôme initial.
On répète cette opération dans les étapes suivantes.

… ensuite…

$$\begin{array}{rl|l} 7X^5 + 4X^4 + 2X^3 - X + 5 & X^2 + 2 \\ \hline -7X^5 \quad -14X^3 & 7X^3 + 4X^2 \\ \hline 4X^4 - 12X^3 - X + 5 & \\ -4X^4 \quad -8X^2 & \\ \hline -12X^3 - 8X^2 - X + 5 & \end{array}$$

… et enfin…

$$\begin{array}{rl|l}
7X^5+4X^4+2X^3 & -X+5 & X^2+2 \\
\cline{3-3}
-7X^5 \quad -14X^3 & & 7X^3+4X^2-12X-8 \\
\cline{1-2}
4X^4-12X^3 & -X+5 & \\
-4X^4 \quad -8X^2 & & \\
\cline{1-2}
-12X^3-8X^2 & -X+5 & \\
+12X^3 \quad +24X & & \\
\cline{1-2}
-8X^2+23X & +5 & \\
+8X^2 & +16 & \\
\cline{1-2}
23X & +21 &
\end{array}$$

Le quotient de notre division est $7X^3+4X^2-12X-8$, et son reste est $23X+21$.

Corollaire (Divisibilité dans $\mathbb{R}[X]$ et divisibilité dans $\mathbb{C}[X]$) Soient $A, B \in \mathbb{R}[X]$ — à coefficients **réels**, attention.

(i) Si $B \neq 0$, la division euclidienne de A par B est la même dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

(ii) A divise B dans $\mathbb{R}[X]$ si et seulement si A divise B dans $\mathbb{C}[X]$.

✌ ✌ ✌ **Explication** Quand on divise deux polynômes à coefficients **réels** A et B l'un par l'autre, disons A par B, on a a priori un vrai choix à faire : effectuer cette division dans $\mathbb{R}[X]$ — quotient et reste dans $\mathbb{R}[X]$ — ou l'effectuer dans $\mathbb{C}[X]$ — quotient et reste dans $\mathbb{C}[X]$. Le théorème affirme justement que la distinction $\mathbb{R}[X]/\mathbb{C}[X]$ n'est ici d'aucun intérêt.

Démonstration

(i) La division euclidienne de A par B dans $\mathbb{R}[X]$ est aussi une division euclidienne de A par B dans $\mathbb{C}[X]$. Par unicité de la division euclidienne, on en déduit que cette division euclidienne est tout simplement **la** division euclidienne de A par B dans $\mathbb{C}[X]$, de sorte que les deux divisions euclidiennes coïncident.

(ii) Dire que A divise B dans $\mathbb{R}[X]$ (resp. $\mathbb{C}[X]$), c'est dire que le reste de la division euclidienne de A par B dans $\mathbb{R}[X]$ (resp. $\mathbb{C}[X]$) est nul. Les deux divisions euclidiennes coïncidant d'après (i), leurs restes sont égaux. Voilà pourquoi A divise B dans $\mathbb{R}[X]$ si et seulement si A divise B dans $\mathbb{C}[X]$. ■

3 Racines d'un polynôme

3.1 Fonctions polynomiales

Définition (Evaluation polynomiale et fonction polynomiale)

- Soient $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On note $P(\lambda)$ l'élément de $\mathbb{K}$ défini par : $P(\lambda) = \sum_{k=0}^{\infty} a_k \lambda^k$ (somme **finie**).
- L'application $\widetilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x) \end{array} \right.$ est appelée la *fonction polynomiale associée à P*.
- L'application $\left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \widetilde{P} \end{array} \right.$ est un morphisme d'anneaux qui préserve la composition. Pour tous $P, Q \in \mathbb{K}[X]$:

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \qquad \widetilde{PQ} = \widetilde{P}\widetilde{Q} \qquad \text{et} \qquad \widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}.$$

✎ ✎ ✎ **En pratique (Algorithme de Horner)** L'*algorithme de Horner* est un algorithme de calcul rapide des valeurs d'un polynôme. Précisément, soient $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Objectif de l'algorithme : calculer $P(\lambda)$.

- A première vue l'affaire est simple : on calcule les puissances de λ, on les multiplie par les coefficients de P et on additionne. Mais ce travail est-il long ? Le calcul de λ^k requiert $(k-1)$ multiplications pour tout $k \in \mathbb{N}^*$, donc celui de $a_k\lambda^k$ requiert k multiplications. Il reste ensuite à additionner ce petit monde avec n additions. Au total, cette méthode (très) naïve de calcul nous aura coûté $n + \sum_{k=1}^{n} k = n + \frac{n(n+1)}{2} = \frac{n(n+3)}{2} \underset{n\to\infty}{\sim} \frac{n^2}{2}$ additions et multiplications confondues.

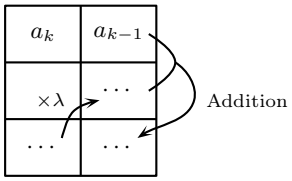
- L'algorithme de Horner repose sur l'identité : $$P=\sum_{k=0}^{n}a_kX^k=\Big(\Big(\dots\big((a_nX+a_{n-1})X+a_{n-2}\big)X+\dots\Big)X+a_1\Big)X+a_0$$

  qui se lit « depuis le milieu » : pour calculer $P(\lambda)$, on peut commencer par calculer $a_n\lambda+a_{n-1}$, puis $(a_n\lambda+a_{n-1})\lambda+a_{n-2}$, etc. Chaque étape requiert une multiplication et une addition. En tout, l'algorithme de Horner exige donc la mise en œuvre de $2n$ additions ou multiplications. C'est **infiniment** moins que la méthode naïve car $2n \underset{n\to\infty}{=} o(n^2)$.

- On présente souvent la mise en œuvre de cet algorithme au moyen d'un tableau :

a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$P(\lambda)$

rempli selon le principe suivant :



3.2 Racines

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 $\partial^\circ R<1$, donc en fait R est un polynôme constant. Evaluons en λ : $P(\lambda)=(\lambda-\lambda)Q(\lambda)+R(\lambda)=R$. ■

Définition (Racine) Soient $P\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$. Les assertions suivantes sont équivalentes :

(i) $P(\lambda)=0$. (ii) P est divisible par $(X-\lambda)$ dans $\mathbb{K}[X]$.

On dit dans ce cas que λ est une *racine de P (dans $\mathbb{K}$)*.

Démonstration Conséquence immédiate du théorème précédent. ■

✖✖✖ **Attention !** La précision « racine **dans** $\mathbb{K}$ » n'est pas superflue. Par exemple, 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 $-i$.

3.3 Multiplicité

Définition (Multiplicité) Soient $P\in\mathbb{K}[X]$ **non nul** et $\lambda\in\mathbb{K}$.

- L'ensemble $\Big\{k\in\mathbb{N}/\quad (X-\lambda)^k \text{ divise } P\Big\}$ possède un plus grand élément m qu'on appelle la *multiplicité de λ dans P* ou l'*ordre de 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 de multiplicité 1 est dite *simple*; de multiplicité 2, *double*.

- Plus concrètement, m est caractérisé par les propositions suivantes :

(i) P est divisible par $(X-\lambda)^m$ mais PAS par $(X-\lambda)^{m+1}$.

(ii) Il existe $Q\in\mathbb{K}[X]$ tel que $P=(X-\lambda)^mQ$ et $Q(\lambda)\neq 0$.

Démonstration Supposons $P\neq 0$ et notons $\mathcal{M}$ l'ensemble $\Big\{k\in\mathbb{N}/\quad (X-\lambda)^k \text{ divise } P\Big\}$. Pour montrer que $\mathcal{M}$ possède un plus grand élément, il nous suffit de montrer que c'est une partie non vide majorée de $\mathbb{N}$.

1) $\mathcal{M}$ une partie non vide de $\mathbb{N}$ car $(X-\lambda)^0=1$ divise P.

2) Montrons que $\partial^\circ P$ majore $\mathcal{M}$. Soit $k\in\mathbb{N}$ pour lequel $(X-\lambda)^k$ divise P. Alors $P=(X-\lambda)^kQ$ pour un certain $Q\in\mathbb{K}[X]$. Or $P\neq 0$ donc $Q\neq 0$, donc $\partial^\circ Q\geqslant 0$, et enfin : $k\leqslant\partial^\circ Q+k=\partial^\circ P$. ■

Théorème (Formules de Taylor, version polynomiale) Soient $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$.

$$P = \sum_{k=0}^{\infty} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k \qquad \text{et} \qquad P(X+\lambda) = \sum_{k=0}^{\infty} \frac{P^{(k)}(\lambda)}{k!} X^k.$$

Démonstration Nous devons surtout montrer que $P = \sum_{k=0}^{\infty} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$. L'autre formule s'en déduit par composition par $X+\lambda$. Introduisons les coefficients de P : $P = \sum_{k=0}^{\infty} a_k X^k$.

$$\begin{aligned} P &= \sum_{k=0}^{\infty} a_k X^k = \sum_{k=0}^{\infty} a_k \big((X-\lambda)+\lambda\big)^k = \sum_{k=0}^{\infty} a_k \sum_{i=0}^{k} \binom{k}{i} (X-\lambda)^i \lambda^{k-i} = \sum_{i=0}^{\infty} \frac{(X-\lambda)^i}{i!} \sum_{k=i}^{\infty} a_k \, \frac{k!}{(k-i)!} \, \lambda^{k-i} \\ &= \sum_{i=0}^{\infty} \frac{(X-\lambda)^i}{i!} \sum_{k=0}^{\infty} a_k \times k(k-1)(k-2)\dots(k-i+1)\lambda^{k-i} = \sum_{i=0}^{\infty} \frac{(X-\lambda)^i}{i!} \sum_{k=0}^{\infty} a_k \big(X^k\big)^{(i)}(\lambda) \\ &= \sum_{i=0}^{\infty} \frac{(X-\lambda)^i}{i!} \left(\sum_{k=0}^{\infty} a_k X^k\right)^{(i)}(\lambda) = \sum_{i=0}^{\infty} \frac{(X-\lambda)^i}{i!} P^{(i)}(\lambda) = \sum_{k=0}^{\infty} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k. \end{aligned}$$

■

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

(i) λ est de multiplicité m dans P.

(ii) $P^{(i)}(\lambda) = 0$ pour tout $i \in [\![0, m-1]\!]$ MAIS $P^{(m)}(\lambda) \neq 0$.

Démonstration

(i) $\Longrightarrow$ (ii) Supposons λ de multiplicité m dans P, i.e. que $P = (X-\lambda)^m Q$ pour un certain $Q \in \mathbb{K}[X]$ tel que $Q(\lambda) \neq 0$. D'après la formule de Taylor :

$$\begin{aligned} P = \sum_{i=0}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^i &= \overbrace{\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^i}^{\text{degré strictement inférieur à } m} + (X-\lambda)^m \sum_{i=m}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^{i-m} \\ &= 0 + (X-\lambda)^m \quad Q. \end{aligned}$$

Par unicité de la division euclidienne de P par $(X-\lambda)^m$: $\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^i = 0$, donc après composition à droite par $X+\lambda$: $\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!} X^i = 0$. Enfin, par identification, $P^{(i)}(\lambda) = 0$ pour tout $i \in [\![0, m-1]\!]$. Ensuite, toujours par unicité de la division euclidienne : $Q = \sum_{i=m}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^{i-m}$. Comme $Q(\lambda) \neq 0$, on obtient $\frac{P^{(m)}(\lambda)}{m!} \neq 0$ après évaluation en λ, donc enfin $P^{(m)}(\lambda) \neq 0$.

(ii) $\Longrightarrow$ (i) Supposons que $P(\lambda) = P'(\lambda) = \dots = P^{(m-1)}(\lambda) = 0$ mais que $P^{(m)}(\lambda) \neq 0$.
La formule de Taylor en tête, posons $Q = \sum_{i=m}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^{i-m}$. Alors $Q(\lambda) = \frac{P^{(m)}(\lambda)}{m!} \neq 0$ et :

$$P = \sum_{i=0}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^i = \sum_{i=0}^{m-1} \underbrace{\frac{P^{(i)}(\lambda)}{i!}}_{=0} (X-\lambda)^i + (X-\lambda)^m \sum_{i=m}^{\infty} \frac{P^{(i)}(\lambda)}{i!} (X-\lambda)^{i-k} = (X-\lambda)^m Q,$$

donc λ est de multiplicité m dans P. ■

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

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

3.4 Nombre de racines

Théorème (Factorisation « par les racines ») Soient $P \in \mathbb{K}[X]$ non nul et $\lambda_1, \lambda_2, \dots, \lambda_r$ des racines distinctes de P de multiplicités respectives $m_1, m_2, \dots, m_r$. Alors $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_r)^{m_r}$ divise P. En particulier : $\sum_{k=1}^{r} m_k \leqslant \partial^\circ P$.

Démonstration Montrons que pour tout $k \in [\![1, r-1]\!]$, $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_k)^{m_k}$ 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 $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_k)^{m_k}$ divise P.

  1) Alors $P = (X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_k)^{m_k}A$ pour un certain $A \in \mathbb{K}[X]$.

  2) Si α désigne la multiplicité de λ_{k+1} dans A, $A = (X-\lambda_{k+1})^\alpha B$ pour un certain $B \in \mathbb{K}[X]$ avec $B(\lambda_{k+1}) \neq 0$. En outre $(X-\lambda_{k+1})^\alpha$ divise A, donc P, donc $\alpha \leqslant m_{k+1}$.

  3) 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 $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_k)^{m_k}(X-\lambda_{k+1})^\alpha B = (X-\lambda_{k+1})^{m_{k+1}}C$. Divisons cette égalité par $(X-\lambda_{k+1})^\alpha$ grâce à l'intégrité de $\mathbb{K}[X]$:

  $$(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_k)^{m_k}B = (X-\lambda_{k+1})^{m_{k+1}-\alpha}C.$$

  Le polynôme de gauche n'admettant pas λ_{k+1} pour racine, il en est de même du polynôme de droite, donc $\alpha = m_{k+1}$. Bref, $(X-\lambda_{k+1})^{m_{k+1}}$ divise A, donc $(X-\lambda_1)^{m_1}(X-\lambda_2)^{m_2}\dots(X-\lambda_{k+1})^{m_{k+1}}$ divise P. ■

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 de racines comptées avec multiplicité)

- Un polynôme **non nul** P possède au plus $\partial^\circ P$ racines **comptées avec multiplicité**.
- En particulier, seul le polynôme nul possède une infinité de racines.

✖✖✖ **Attention !** Un polynôme de degré n n'a pas forcément exactement n racines comptées avec multiplicité. Nous verrons que c'est le cas si $\mathbb{K} = \mathbb{C}$ mais pas si $\mathbb{K} = \mathbb{R}$. Par exemple, $X^2+1 \in \mathbb{R}[X]$ est de degré 2 mais n'a aucune racine dans $\mathbb{R}$.

Exemple La fonction sinus n'est pas polynomiale, car elle s'annule une infinité de fois sans être identiquement nulle.

Théorème (Identification polynôme/fonction polynomiale) Le morphisme d'anneaux $\left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \widetilde{P} \end{array} \right.$ qui, à tout polynôme, associe la fonction polynomiale associée, est injectif.

Deux fonctions polynomiales égales sur $\mathbb{K}$ sont donc associées à un seul et même polynôme. On peut ainsi identifier tout polynôme à sa fonction polynomiale.

✎✎✎ **En pratique** Bien qu'on puisse identifier un polynôme et sa fonction polynomiale, je vous conseille de bien distinguer ces deux objets. A l'écrit comme à l'oral, vous montrerez ainsi aux gens qui vous corrigent que vous avez compris qu'il y a une vraie différence conceptuelle entre ces notions.

Démonstration Nous devons montrer que le morphisme considéré est injectif, i.e. que son noyau ne contient que le polynôme nul. Soit $P \in \mathbb{K}[X]$ pour lequel $\widetilde{P}$ est l'application constante égale à 0 sur $\mathbb{K}$. Alors pour tout $\lambda \in \mathbb{K}$, $P(\lambda) = \widetilde{P}(\lambda) = 0$ donc λ est une racine de P. Il apparaît ainsi que tout élément de $\mathbb{K}$ est une racine de P. Or nous travaillons avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$, donc P possède une infinité de racines. Comme voulu $P = 0$. ■

3.5 Polynômes scindés et relations coefficients/racines

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

Dire que P est scindé sur $\mathbb{K}$ revient donc à dire que P est de la forme : $P = A\prod_{k=1}^{r}(X-\lambda_k)^{\alpha_k}$, où $\lambda_1, \lambda_2, \dots, \lambda_r$ sont les racines distinctes de P dans $\mathbb{K}$, de multiplicités respectives $\alpha_1, \alpha_2, \dots, \alpha_r$, et où A est son coefficient dominant.

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

Exemple Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$. Vous devez connaître les deux identités suivantes :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n}(X-\omega) = \prod_{k=0}^{n-1}\left(X - e^{\frac{2ik\pi}{n}}\right) \qquad \text{et} \qquad \sum_{k=0}^{n-1} X^k = \prod_{\omega \in \mathbb{U}_n \smallsetminus \{1\}}(X-\omega) = \prod_{k=1}^{n-1}\left(X - e^{\frac{2ik\pi}{n}}\right).$$

En effet Le polynôme X^n-1 possède exactement n racines distinctes, à savoir les $e^{\frac{2ik\pi}{n}}$, k décrivant $[\![0, n-1]\!]$. La première formule en découle. Pour la deuxième, il suffit de simplifier par $X-1$ dans les deux membres de la première par intégrité de $\mathbb{K}[X]$. Notez bien qu'on divise ici par le **polynôme** $X-1$, qui **n'est pas** une **fonction**. Si les polynômes étaient des fonctions, on ne pourrait diviser par $X-1$ que pour $X \neq 1$ et le cas $X = 1$ mériterait un traitement à part. Rappelons que X n'est pas un nombre !

Théorème (Relations coefficients/racines) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ scindé de degré n. On note $\lambda_1, \lambda_2, \dots, \lambda_n$ les racines de P comptées avec multiplicité (éventuellement répétées). Pour tout $k \in [\![1, n]\!]$, on pose : $\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n} \lambda_{i_1}\lambda_{i_2}\dots\lambda_{i_k}$.

Alors pour tout $k \in [\![1, n]\!]$: $\sigma_k = (-1)^k \dfrac{a_{n-k}}{a_n}$.

✌✌✌ **Explication**

- Ce théorème ne nous permet pas de calculer les racines de P à partir de ses coefficients — ce serait trop beau — mais il nous permet de le faire pour certaines fonctions $\sigma_1, \sigma_2, \dots, \sigma_n$ des racines, appelées les *fonctions symétriques élémentaires de* $\lambda_1, \lambda_2, \dots, \lambda_n$ — symétriques parce qu'elles ne dépendent pas de l'ordre dans lequel on a rangé $\lambda_1, \lambda_2, \dots, \lambda_n$. 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 $\sigma_4 = \lambda_1\lambda_2\lambda_3\lambda_4$.

- Pour $n = 2$, le résultat est connu : la somme des racines du polynôme aX^2+bX+c $(a \neq 0)$ vaut $-\dfrac{b}{a}$ et leur produit $\dfrac{c}{a}$.

Démonstration Tout repose sur une identification des coefficients de P exprimés de deux façons différentes.

Première expression, triviale : $P = \sum_{k=0}^{n} a_k X^k$.

Seconde expression, moins triviale : $P = a_n\prod_{i=1}^{n}(X-\lambda_i) = a_n\Big(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \sigma_3 X^{n-3} + \dots + (-1)^n\sigma_n\Big)$.

Pour saisir intuitivement le sens de cette seconde expression, calculez le coefficient de degré n dans $\prod_{i=1}^{n}(X-\lambda_i)$, puis celui de degré $(n-1)$, puis celui de degré $(n-2)$, etc. Vous trouverez 1, $-\sigma_1$, σ_2, $-\sigma_3$, etc. Finalement, par identification : $a_{n-1} = -a_n\sigma_1$, $a_{n-2} = a_n\sigma_2$, $a_{n-3} = -a_n\sigma_3$, … $a_0 = (-1)^n a_n\sigma_n$. ■

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 $\prod_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = \prod_{\omega \in \mathbb{U}_n}\omega = (-1)^{n+1}$.

En effet Conservons les notations σ_1 et σ_n du théorème pour le polynôme scindé X^n-1. Alors $\sigma_1 = \sum_{\omega \in \mathbb{U}_n}\omega$ et $\sigma_n = \prod_{\omega \in \mathbb{U}_n}\omega$. Les relations coefficients/racines nous donnent exactement le résultat annoncé.

Exemple On admet momentanément que le polynôme X^3-2X+5 possède trois racines complexes x, y et z 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 $X^3-4X^2+4X-25$.

En effet 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 alors $\sigma_1=x+y+z$, $\sigma_2=xy+yz+zx$ et $\sigma_3=xyz$. Les relations coefficients/racines du polynôme X^3-2X+5 s'écrivent alors : $\sigma_1=0$, $\sigma_2=-2$ 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 $x^2y^2+y^2z^2+z^2x^2=(xy+yz+zx)^2-2\big(xy\times yz+yz\times zx+zx\times xy\big)=\sigma_2^2-2xyz(x+y+z)=\sigma_2^2-2\sigma_1\sigma_3=4$.
Comme annoncé : $\big(X-x^2\big)\big(X-y^2\big)\big(X-z^2\big)=X^3-4X^2+4X-25$.

Exemple Le système $\bigstar\ \begin{cases} x+y+z=1 \\ x^2+y^2+z^2=21 \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=1 \end{cases}$ d'inconnue $(x,y,z)\in\big(\mathbb{C}^*\big)^3$ possède six solutions :

$$\big(1,\sqrt{10},-\sqrt{10}\big),\quad \big(\sqrt{10},-\sqrt{10},1\big),\quad \big(-\sqrt{10},1,\sqrt{10}\big),\quad \big(1,-\sqrt{10},\sqrt{10}\big),\quad \big(-\sqrt{10},\sqrt{10},1\big)\quad\text{et}\quad \big(\sqrt{10},1,-\sqrt{10}\big).$$

En effet Soit $(x,y,z)\in\big(\mathbb{C}^*\big)^3$. On pose : $P=(X-x)(X-y)(X-z)$, $\sigma_1=x+y+z$, $\sigma_2=xy+yz+zx$ et $\sigma_3=xyz$. Alors en vertu des relations coefficients/racines : $P=X^3-\sigma_1X^2+\sigma_2X-\sigma_3$. Remarquons en outre que :

$$x^2+y^2+z^2=(x+y+z)^2-2(xy+yz+zx)=\sigma_1^2-2\sigma_2 \qquad\text{et}\qquad \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{xy+yz+zx}{xyz}=\frac{\sigma_2}{\sigma_3}.$$

Après ces préparatifs, nous pouvons attaquer la résolution du système proposé :

$$\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=21 \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=1 \end{cases} \iff \begin{cases} \sigma_1=1 \\ \sigma_1^2-2\sigma_2=21 \\ \dfrac{\sigma_2}{\sigma_3}=1 \end{cases} \iff \begin{cases} \sigma_1=1 \\ \sigma_2=-10 \\ \sigma_3=-10 \end{cases} \iff P=X^3-X^2-10X+10$$

$$\iff x,y\text{ et }z\text{ sont toutes les racines du polynôme } X^3-X^2-10X+10.$$

Or ce polynôme se factorise aisément : $X^3-X^2-10X+10=(X-1)(X^2-10)=(X-1)\big(X-\sqrt{10}\big)\big(X+\sqrt{10}\big)$.
Finalement, les triplets solutions du système $\bigstar$ sont tous les triplets qu'on peut former à partir des réels 1, $\sqrt{10}$ et $-\sqrt{10}$ en les permutant.

4 Arithmétique dans $\mathbb{K}[X]$

Définition (Diviseur commun, multiple commun) Soient $A,B\in\mathbb{K}[X]$.

- On appelle *diviseur commun de A et B* tout polynôme $D\in\mathbb{K}[X]$ qui est à la fois diviseur de A et diviseur de B.
- On appelle *multiple commun de A et B* tout polynôme $M\in\mathbb{K}[X]$ qui est à la fois multiple de A et multiple de B.

4.1 PGCD

Définition (PGCD) Soient $A,B\in\mathbb{K}[X]$. On appelle *plus grand commun diviseur* (PGCD) *de A et B* tout polynôme $D\in\mathbb{K}[X]$ tel que :

- D est un diviseur commun de A et B : $D|A$ et $D|B$;
- D est un multiple de tout diviseur commun de A et B : $\forall\Delta\in\mathbb{K}[X],\quad \Big(\Delta|A \text{ et } \Delta|B\Big) \implies \Delta|D$.

Un PGCD de deux polynômes existe-t-il toujours ? Si oui, est-il unique ? Nous énonçons ci-après deux théorèmes essentiels. Tous deux seront démontrés simultanément au sein d'une preuve unique.

Théorème (Existence et « unicité » du PGCD) Soient $A, B \in \mathbb{K}[X]$.

- Si $A \neq 0$ ou $B \neq 0$, il existe un unique PGCD **unitaire** de A et B, noté $\text{PGCD}(A,B)$ et appelé **le** PGCD *de A et B*. Il est clair que 0 est l'unique PGCD de 0 et 0 et on peut poser $\text{PGCD}(0,0) = 0$.
- Les autres PGCD de A et B sont tous les $\lambda\,\text{PGCD}(A,B)$, λ décrivant $\mathbb{K}^*$.

✌ ✌ ✌ **Explication** On dira par exemple que $2X$ est **un** PGCD de X et X^2, mais, au choix, que le polynôme unitaire X est **un** ou **le** PGCD de X et X^2.

Théorème (Théorème de Bézout, première partie) Soient $A, B \in \mathbb{K}[X]$.
Il existe des polynômes $U, V \in \mathbb{K}[X]$ tels que $\text{PGCD}(A,B) = AU + BV$. Un tel couple (U,V) est appelé **un** *couple de coefficients de Bézout de* (A,B).

✖ ✖ ✖ **Attention !** Les polynômes U et V ne sont pas du tout uniques.

Démonstration

- Commençons par montrer que les PGCD de A et B, s'ils existent, sont identiques à une constante multiplicative non nulle près, i.e. sont associés. Soient D et D' deux PGCD de A et B. Alors D est un diviseur commun de A et B, donc $D|D'$ puisque D' est un PGCD de A et B. De même D' est un diviseur de A et B, donc $D'|D$ puisque D est un PGCD de A et B. Finalement D et D' sont associés.
- Pour l'existence du PGCD et le théorème de Bézout, commençons par mettre de côté le cas $A = B = 0$. Il est clair dans ce cas que 0 est un PGCD de A et B.

  Nous pouvons désormais supposer $A \neq 0$ ou $B \neq 0$. L'ensemble $\Big\{\partial^\circ(AK+BL)\Big\}_{K,L\in\mathbb{K}[X]} \setminus \{-\infty\}$ est alors une partie non vide de $\mathbb{N}$, donc possède un plus petit élément $d \in \mathbb{N}$. Alors $d = \partial^\circ(AU+BV)$ pour certains polynômes $U, V \in \mathbb{K}[X]$. Posons $D = AU + BV$. Nous allons montrer que D est un PGCD de A et B. Cela montrera en même temps le théorème de Bézout puisque par définition $D = AU + BV$ avec $U, V \in \mathbb{K}[X]$.

  1) Montrons que D divise à la fois A et B. Il suffit de le prouver pour A par symétrie des rôles de A et B. La division euclidienne de A par D s'écrit $A = DQ + R$ où $Q, R \in \mathbb{K}[X]$ et $\partial^\circ R < d$. Alors $\partial^\circ R \in \Big\{\partial^\circ(AK+BL)\Big\}_{K,L\in\mathbb{K}[X]}$ car $R = A - DQ = A - (AU+BV)Q = A(1-UQ) + BVQ$. Or $\partial^\circ R < d$ et d est le plus petit élément de $\Big\{\partial^\circ(AK+BL)\Big\}_{K,L\in\mathbb{K}[X]} \setminus \{-\infty\}$, donc $\partial^\circ R = -\infty$, i.e. $R = 0$. Bref, $A = DQ$, i.e. D divise A.

  2) Soit $\Delta \in \mathbb{K}[X]$ divisant à la fois A et B. Alors Δ divise D puisque $D = AU + BV$. ■

La preuve précédente a ceci d'inconfortable qu'elle ne nous explique pas comment calculer le PGCD de deux polynômes, ni comment calculer les deux polynômes U et V du théorème de Bézout. Nous présentons ci-après deux algorithmes de calcul adaptés à ces questions : l'*algorithme d'Euclide* et l'*algorithme de Bézout*.

Lemme (Idée fondamentale de l'algorithme d'Euclide) Soient $A, B \in \mathbb{K}[X]$, $B \neq 0$ et R le reste de la division euclidienne de A par B. Alors $\text{PGCD}(A,B) = \text{PGCD}(B,R)$.

✎ ✎ ✎ **En pratique (Algorithme d'Euclide)**

- Soient $A, B \in \mathbb{K}[X]$. L'*algorithme d'Euclide* va nous permettre de calculer rapidement le PGCD de A et B. Tout d'abord, $\text{PGCD}(0,0) = 0$. Comme de plus $\text{PGCD}(A,B) = \text{PGCD}(B,A)$, nous pouvons supposer $\partial^\circ B \leqslant \partial^\circ A$ et $A \neq 0$. On définit alors les polynômes $R_0, R_1, R_2 \ldots$ de la façon suivante :

  1) on commence par poser $R_0 = A$ et $R_1 = B$;

  2) ensuite, k désignant un entier naturel, tant que $R_{k+1} \neq 0$, i.e. $\partial^\circ R_{k+1} \neq -\infty$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} — dans ce cas $\partial^\circ R_{k+2} < \partial^\circ R_{k+1}$.

  A l'issue de cette construction : $\partial^\circ R_0 \geqslant \partial^\circ R_1 > \partial^\circ R_2 > \partial^\circ R_3 > \ldots$ Or il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\partial^\circ R_0$, donc forcément $\partial^\circ R_N = -\infty$ pour un certain $N \in \mathbb{N}^*$, i.e. $R_N = 0$. Alors R_{N-1} est le **dernier reste non nul** de la suite $R_0, R_1, R_2 \ldots$ et en vertu de l'idée fondamentale de l'algorithme d'Euclide :

$$\text{PGCD}(A,B) = \text{PGCD}(R_0,R_1) = \text{PGCD}(R_1,R_2) = \ldots = \text{PGCD}(R_{N-1},R_N) = \text{PGCD}(R_{N-1},0) = R_{N-1}^\circ,$$

  où R_{N-1}° est le polynôme R_{N-1} rendu unitaire par division par son coefficient dominant. Bref, le PGCD de A et B est tout simplement le **dernier reste non nul** R_{N-1} (**rendu unitaire**) de la suite des restes successifs $R_0, R_1, R_2 \ldots$

- Déterminons par exemple le PGCD de $A = X^4 + 7X^3 + 17X^2 + 17X + 6$ et $B = X^3 + X^2 - 4X - 4$. On commence par effectuer la division euclidienne de A par B, puisque $\partial^\circ B \leqslant \partial^\circ A$: $A = (X+6)B + (15X^2 + 45X + 30)$.
  On poursuit avec la division euclidienne de B par $15X^2 + 45X + 30 = 15(X^2 + 3X + 2)$. Mais pour éviter que les calculs soient pénibles, on peut plutôt diviser B par $X^2 + 3X + 2$: $B = (X-2) \times (X^2 + 3X + 2) + 0$.
  Le dernier reste non nul obtenu est $X^2 + 3X + 2$ (peu importe le facteur 15, puisqu'on veut des PGCD unitaires).
  Conclusion : $\mathrm{PGCD}(A, B) = X^2 + 3X + 2$.

✎✎✎ **En pratique (Algorithme de Bézout)** Nous allons, sur un exemple, retrouver l'idée du calcul des coefficients de Bézout que nous avons étudiée dans le chapitre d'arithmétique dans $\mathbb{Z}$.

Cherchons par exemple le PGCD des polynômes $A = 6X^4 + 8X^3 - 7X^2 - 5X - 2$ et $B = 6X^3 - 4X^2 - X - 1$ ainsi qu'une relation de Bézout associée. Tout commence avec les divisions euclidiennes successives de l'algorithme d'Euclide, dont nous notons $R_0, R_1, R_2, \ldots$ les restes successifs à partir de $R_0 = A$ et $R_1 = B$:

$$\overbrace{6X^4 + 8X^3 - 7X^2 - 5X - 2}^{R_0} = (X+2) \times \overbrace{(6X^3 - 4X^2 - X - 1)}^{R_1} + \overbrace{2X^2 - 2X}^{R_2},$$

$$\overbrace{6X^3 - 4X^2 - X - 1}^{R_1} = (3X+1) \times \overbrace{(2X^2 - 2X)}^{R_2} + \overbrace{X - 1}^{R_3},$$

$$\overbrace{2X^2 - 2X}^{R_2} = 2X \times \overbrace{(X-1)}^{R_3} + \overbrace{0}^{R_4}.$$

Le dernier reste non nul est $X - 1$ et il est unitaire, c'est lui le PGCD de A et B. Finalement :

$$\begin{aligned}
\mathrm{PGCD}(A, B) = \overbrace{X-1}^{R_3} &= \overbrace{6X^3 - 4X^2 - X - 1}^{R_1} - (3X+1) \times \overbrace{(2X^2 - 2X)}^{R_2} \\
&= \overbrace{B}^{R_1} - (3X+1) \times \big(\overbrace{A}^{R_0} - (X+2) \times \overbrace{B}^{R_1} \big) \qquad \text{(on élimine } R_2\text{)} \\
&= -(3X+1) \times \overbrace{A}^{R_0} + (3X^2 + 7X + 3) \times \overbrace{B}^{R_1}. \qquad \text{La voilà, notre identité de Bézout.}
\end{aligned}$$

Théorème (Propriétés du PGCD) Soient $A, B \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ **unitaire**.

$$\mathrm{PGCD}(AP, BP) = P \times \mathrm{PGCD}(A, B).$$

✌✌✌ **Explication** En arithmétique des entiers relatifs, la formule « $\mathrm{PGCD}(ak, bk) = k\,\mathrm{PGCD}(a, b)$ » est vraie si $k \geqslant 0$ — ou on écrit $|k|$ à la place de k. Dans le contexte des polynômes, la condition « P est unitaire » remplace la condition « $k \geqslant 0$ ».

4.2 Polynômes premiers entre eux

Définition (Polynômes premiers entre eux) Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont *premiers entre eux* si leurs seuls diviseurs communs sont les polynômes constants non nuls, i.e. si leur PGCD est égal à 1.

Théorème (Théorème de Bézout, deuxième partie) Soient $A, B \in \mathbb{K}[X]$. Les assertions suivantes sont équivalentes :

(i) A et B sont premiers entre eux. (ii) Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Théorème (Théorème de Gauss) Soient $A, B, C \in \mathbb{K}[X]$. Si $A|BC$ et si A et B sont premiers entre eux, alors $A|C$.

Corollaire (Divisibilité par un produit) Soient $A, B, P \in \mathbb{K}[X]$. Si $A|P$, si $B|P$ et si A et B sont premiers entre eux, alors $AB|P$.

✖✖✖ **Attention !** Il est impératif de supposer ici A et B premiers entre eux. En effet, pour $A = B = P = X$, A et B divisent P mais AB ne divise pas P, et ce n'est pas étonnant puisque A et B ne sont pas premiers entre eux.

4.3 PPCM

Définition (PPCM) Soient $A, B \in \mathbb{K}[X]$. On appelle *plus petit commun multiple* (PPCM) *de A et B* tout polynôme $M \in \mathbb{K}[X]$ tel que :

- M est un multiple commun de A et B : $\quad A|M \quad$ et $\quad B|M \quad$;
- M est un diviseur de tout multiple commun de A et B : $\quad \forall N \in \mathbb{K}[X], \quad \Big(A|N \ \text{ et } \ B|N\Big) \quad \Longrightarrow \quad M|N.$

Un PPCM de deux polynômes existe-t-il toujours ? Si oui, est-il unique ? Le théorème suivant répond à ces questions.

Théorème (Existence et « unicité » du PPCM) Soient $A, B \in \mathbb{K}[X]$.

- Si $A \neq 0$ et $B \neq 0$, il existe un unique PPCM **unitaire** de A et B, noté $\text{PPCM}(A, B)$ et appelé **le** PPCM *de A et B*. Si $A = 0$ ou $B = 0$, alors 0 est un PPCM de A et B et on pose $\text{PPCM}(A, B) = 0$.
- Les autres PPCM de A et B sont tous les λ $\text{PPCM}(A, B)$, λ décrivant $\mathbb{K}^*$.

De plus, AB et $\text{PGCD}(A, B)$ $\text{PPCM}(A, B)$ sont associés, i.e. égaux à une constante multiplicative non nulle près.

Théorème (Propriétés du PPCM) Soient $A, B \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ **unitaire**.

$$\text{PPCM}(AP, BP) = P \times \text{PPCM}(A, B).$$

4.4 Polynômes irréductibles

Définition (Polynôme irréductible) Soit $P \in \mathbb{K}[X]$. On dit que P est *irréductible* (*dans* $\mathbb{K}[X]$) si P n'est **pas constant** et si ses seuls diviseurs sont les λ et les λP, λ décrivant $\mathbb{K}^*$.

✌ ✌ ✌ **Explication** Les polynômes irréductibles sont l'analogue polynomial des nombres premiers dans $\mathbb{Z}$ et des particules élémentaires en physique. Ils vont nous servir à casser tout polynôme en petits morceaux que l'on ne peut pas casser plus.

✖ ✖ ✖ **Attention !** La précision « irréductible **dans** $\mathbb{K}[X]$ » n'est pas superflue. Nous allons voir dans un instant que le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$ car $X^2 + 1 = (X + i)(X - i)$.

Exemple Tout polynôme de degré 1 est irréductible.

En effet Soit $P \in \mathbb{K}[X]$ de degré 1. Soit en outre D un diviseur de P et $A \in \mathbb{K}[X]$ tel que $P = AD$. Alors A est non nul donc $\partial^\circ A \geqslant 0$, de sorte que $\partial^\circ D \leqslant \partial^\circ P$. Ainsi D est de degré 0 ou 1.

- Si $\partial^\circ D = 0$, D est un polynôme constant non nul.
- Si $\partial^\circ D = 1$, alors $\partial^\circ A = 0$, i.e. A est un polynôme constant non nul a. Aussitôt D s'écrit $\dfrac{1}{a}\, P$.

Tout ceci montre bien que P est irréductible dans $\mathbb{K}[X]$.

Exemple Tout polynôme de degré 2 **sans racine** dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$ — par exemple, $X^2 + 1$ dans $\mathbb{R}[X]$.

En effet Soit $P \in \mathbb{K}[X]$ de degré 2 sans racine dans $\mathbb{K}$. Soit en outre D un diviseur de P. Alors D est de degré 0, 1 ou 2.

- Si $\partial^\circ D = 0$, D est un polynôme constant non nul.
- Si $\partial^\circ D = 2$, alors $\partial^\circ A = 0$, i.e. A est un polynôme constant non nul a. Aussitôt D s'écrit $\dfrac{1}{a}\, P$.
- Enfin, D peut-il être de degré 1 ? Si c'était le cas, D serait de la forme $aX + b$ pour certains $a, b \in \mathbb{K}$ avec $a \neq 0$, de sorte que $-\dfrac{b}{a}$ serait une racine de P, contrairement à nos hypothèses.

Tout ceci montre bien que P est irréductible dans $\mathbb{K}[X]$.

Théorème (Existence et unicité de la décomposition en produit de polynômes irréductibles unitaires) Soient $P \in \mathbb{K}[X]$ non constant. Il existe un unique entier $r \in \mathbb{N}^*$, des polynômes irréductibles unitaires $P_1, P_2, \dots, P_r$ uniques à l'ordre près associés respectivement à des entiers naturels non nuls $m_1, m_2, \dots, m_r$, et enfin un unique élément $\lambda \in \mathbb{K}^*$ tels que :

$$P = \lambda P_1^{m_1} P_2^{m_2} \dots P_r^{m_r}.$$

Les polynômes $P_1, P_2, \dots, P_r$ sont tous les polynômes irréductibles unitaires qui divisent P. Pour tout $i \in [\![1, r]\!]$, $P_i^{m_i}$ est la plus grande puissance de P_i qui divise P et m_i est appelé la *multiplicité de P_i dans P* ou l'*ordre de multiplicité de P_i dans P*.

Par convention, on considère que les polynômes constants non nuls possèdent eux aussi une et une seule décomposition de ce genre avec $r = 0$ — bref, ils sont le « produit de zéro polynôme irréductible unitaire ».

✎✎✎ **En pratique** Quand on connaît la décomposition en produit de polynômes irréductibles unitaires de deux polynômes A et B, on peut déterminer $\mathrm{PGCD}(A, B)$ et $\mathrm{PPCM}(A, B)$ sans utiliser l'algorithme de Bézout. Le principe est le même que dans $\mathbb{Z}$. Par exemple, le PGCD de $A = 2X(X+1)^2(X+2)^3$ et $B = (X-1)X(X+2)^4(X^2+1)$ est $X(X+2)^3$: on conserve, pour chaque facteur irréductible unitaire commun de A et B, la plus grande puissance de ce facteur qui divise à la fois A et B. Pour une raison analogue, le PPCM de A et B est ici $(X-1)X(X+1)^2(X+2)^4(X^2+1)$.

Encore faut-il pouvoir déterminer la décomposition d'un polynôme en produit de polynômes irréductibles unitaires. C'est loin d'être simple en général, voire en un sens parfois impossible.

5 Le théorème de d'Alembert-Gauss

Tout polynôme possède-t-il une racine ? Le résultat suivant est un théorème majeur des mathématiques. On l'appelle aussi parfois le *théorème fondamental de l'algèbre*.

Théorème (Théorème de d'Alembert-Gauss)
Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine **COMPLEXE**.

Démonstration Hors-programme. Les curieux trouveront tout de même une preuve à la fin du chapitre. ■

✖✖✖ **Attention !** Le théorème est faux dans $\mathbb{R}[X]$. Le polynôme $X^2 + 1$, par exemple, n'a pas de racine **réelle**.

Théorème (Polynômes irréductibles de $\mathbb{C}[X]$)

(i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

(ii) Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Démonstration

(i) Soit P un polynôme irréductible de $\mathbb{C}[X]$. Alors P est non constant, donc possède une racine $\lambda \in \mathbb{C}$ d'après le théorème de d'Alembert-Gauss. Par conséquent $X - \lambda$ divise P. Or P est irréductible dans $\mathbb{C}[X]$, donc P et $X - \lambda$ sont associés. Bref, P est de degré 1. La réciproque a déjà été traitée plus haut.

(ii) découle de (i) et du théorème de décomposition en produit de polynômes irréductibles unitaires. ■

Définition (Conjugué d'un polynôme) Soit $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{C}[X]$.

- On appelle *conjugué de P* et on note $\bar{P}$ le polynôme $\sum_{k=0}^{\infty} \bar{a}_k X^k$.
- Pour tout $\lambda \in \mathbb{C}$, la multiplicité de $\bar{\lambda}$ dans $\bar{P}$ est égale à la multiplicité de λ dans P.

En particulier, si $P \in \mathbb{R}[X]$, $\bar{P} = P$. Dans ce cas, pour tout $\lambda \in \mathbb{C}$, λ et $\bar{\lambda}$ ont la même multiplicité dans P.

Démonstration Pour tout $k \in \mathbb{N}$: $\bar{P}^{(k)}(\bar{\lambda}) = \sum_{p=0}^{\infty} \bar{a_p}\bar{\lambda}^p = \overline{\sum_{p=0}^{\infty} a_p\lambda^p} = \overline{P^{(k)}(\lambda)}$. Du coup, pour tout $m \in \mathbb{N}$:

$$\begin{aligned}
\lambda \text{ est de multiplicité } m \text{ dans } P &\iff \Big(\forall k \in [\![0, m-1]\!],\ P^{(k)}(\lambda) = 0\Big) \text{ et } P^{(m)}(\lambda) \neq 0 \\
&\iff \Big(\forall k \in [\![0, m-1]\!],\ \bar{P}^{(k)}(\bar{\lambda}) = 0\Big) \text{ et } \bar{P}^{(m)}(\bar{\lambda}) \neq 0 \\
&\iff \bar{\lambda} \text{ est de multiplicité } m \text{ dans } \bar{P}.
\end{aligned}$$ ■

Théorème (Polynômes irréductibles de $\mathbb{R}[X]$)

(i) Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif (i.e. sans racine réelle).

(ii) Tout polynôme $P \in \mathbb{R}[X]$ possède une unique décomposition de la forme $A\prod_{i=1}^{r}(X-\lambda_i)^{m_i} \times \prod_{j=1}^{s}(X^2+b_jX+c_j)^{n_j}$ dans laquelle :

- A est le coefficient dominant de P ;
- $\lambda_1, \lambda_2, \dots, \lambda_r$ sont les racines réelles distinctes de P et $m_1, m_2, \dots, m_r$ les multiplicités associées ;
- les polynômes $X^2 + b_jX + c_j$ sont distincts et irréductibles dans $\mathbb{R}[X]$ pour tout $j \in [\![1, s]\!]$, avec $n_j \in \mathbb{N}^*$.

Démonstration

(i) Soit P un polynôme irréductible de $\mathbb{R}[X]$. Alors P est non constant et possède donc une racine λ **COMPLEXE** en vertu du théorème de d'Alembert-Gauss.

• Si $\lambda \in \mathbb{R}$, alors $X - \lambda$ divise P dans $\mathbb{R}[X]$. Or P est irréductible dans $\mathbb{R}[X]$, donc P et $X - \lambda$ sont associés et P est de degré 1.

• Si $\lambda \in \mathbb{C} \setminus \mathbb{R}$, alors $\bar{\lambda} \neq \lambda$. Or λ est une racine de P et $P \in \mathbb{R}[X]$, donc $\bar{P} = P$ et $\bar{\lambda}$ est aussi une racine de P. Les polynômes $X - \lambda$ et $X - \bar{\lambda}$ étant premiers entre eux puisque $\bar{\lambda} \neq \lambda$, leur produit $(X-\lambda)(X-\bar{\lambda}) = X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$ divise P. Or $X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2 \in \mathbb{R}[X]$ et P est irréductible dans $\mathbb{R}[X]$, donc P et $X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$ sont associés et P est de degré 2. Pour finir, comme voulu, P est bien sans racine réelle.

(ii) Soit $P \in \mathbb{R}[X]$ non constant. Alors P est scindé **sur $\mathbb{C}$**. De plus, comme $\bar{P} = P$, les racines non réelles de P peuvent être regroupées par paires de conjuguées (avec la même multiplicité) et, comme en (i), le regroupement de deux termes $(X - \lambda)$ et $(X - \bar{\lambda})$ donne un terme $X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$. ■

✎ ✎ ✎ **En pratique** La méthode de l'exemple suivant est à connaître impérativement : la décomposition en produit de polynômes irréductibles unitaires dans $\mathbb{R}[X]$ se calcule à partir des racines complexes (avec multiplicités) par regroupement de chaque racine non réelle avec son conjugué.

Exemple La décomposition de $X^4 + 16$ en produit de polynômes irréductibles unitaires dans $\mathbb{C}[X]$ est :

$$X^4 + 16 = \Big(X - 2e^{-\frac{i\pi}{4}}\Big)\Big(X - 2e^{\frac{i\pi}{4}}\Big)\Big(X - 2e^{-\frac{3i\pi}{4}}\Big)\Big(X - 2e^{\frac{3i\pi}{4}}\Big).$$

Pour la décomposition dans $\mathbb{R}[X]$: $X^4 + 16 = \big(X^2 - 2\sqrt{2}X + 4\big)\big(X^2 + 2\sqrt{2}X + 4\big)$.

En effet

- Commençons par calculer les racines de $X^4 + 16$ dans $\mathbb{C}$. Pour tout $r \in \mathbb{C}$:

$$r^4 + 16 = 0 \iff r^4 = -16 = \Big(2e^{\frac{i\pi}{4}}\Big)^4 \iff \exists\, k \in [\![0, 3]\!],\quad r = 2e^{\frac{i\pi}{4} + \frac{2ik\pi}{4}}.$$

  Les racines de $X^4 + 16$ sont donc $2e^{\frac{i\pi}{4}}$ $(k = 0)$, $2e^{\frac{3i\pi}{4}}$ $(k = 1)$, $2e^{\frac{-3i\pi}{4}}$ $(k = 2)$ et $2e^{\frac{-i\pi}{4}}$ $(k = 3)$. La décomposition de $X^4 + 16$ en produit de polynômes irréductibles unitaires dans $\mathbb{C}[X]$ en découle immédiatement.

- Pour obtenir la décomposition dans $\mathbb{R}[X]$, nous devons regrouper les racines par paires de conjuguées comme dans la preuve précédente :

$$\Big(X - 2e^{-\frac{i\pi}{4}}\Big)\Big(X - 2e^{\frac{i\pi}{4}}\Big) = X^2 - 2\Big(e^{-\frac{i\pi}{4}} + e^{\frac{i\pi}{4}}\Big)X + 4 = X^2 - 4\cos\frac{\pi}{4} \times X + 4 = X^2 - 2\sqrt{2}X + 4$$

  et $\Big(X - 2e^{-\frac{3i\pi}{4}}\Big)\Big(X - 2e^{\frac{3i\pi}{4}}\Big) = X^2 - 2\Big(e^{-\frac{3i\pi}{4}} + e^{\frac{3i\pi}{4}}\Big)X + 4 = X^2 - 4\cos\frac{3\pi}{4} \times X + 4 = X^2 + 2\sqrt{2}X + 4.$

Achevons ce chapitre sur une preuve — hors-programme — du 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 d'abord qu'elle possède un minimum, puis prouver que ce minimum est forcément 0 — ce qui garantira bien l'existence d'une racine.

Introduisons pour le moment les coefficients de P : $P = \sum_{k=0}^{d} a_k X^k$, où $d = \partial^\circ P \geqslant 1$ et $a_d \neq 0$.

- Montrons que $|P|$ possède un minimum dans $\mathbb{C}$. En tout cas, la fonction $|P|$ étant positive, la propriété de la borne inférieure justifie l'existence de $m = \inf_{\mathbb{C}} |P|$. Mais avons-nous là un minimum ?

  1) Pour tout $n \in \mathbb{N}$, $m + \frac{1}{2^n}$ ne minore pas $|P|$, donc $\big|P(z_n)\big| < m + \frac{1}{2^n}$ pour un certain $z_n \in \mathbb{C}$ — et même : $m \leqslant \big|P(z_n)\big| < m + \frac{1}{2^n}$. Le théorème des gendarmes montre aussitôt que $\lim_{n\to\infty} \big|P(z_n)\big| = m$.

  2) Pour tout $z \in \mathbb{C}$: $\big|P(z)\big| = \left|\sum_{k=0}^{d} a_k X^k\right| \geqslant |a_d|.|z|^d - \left|\sum_{k=0}^{d-1} a_k z^k\right| \geqslant |a_d|.|z|^d - \sum_{k=0}^{d-1} |a_k|.|z|^k$. Posons $S = \sum_{k=0}^{d-1} |a_k|$. Alors pour $|z| \geqslant 1$:

  $$\big|P(z)\big| \geqslant |a_d|.|z|^d - \left(\sum_{k=0}^{d-1} |a_k|\right)|z|^{d-1} = |a_d|.|z|^d \left(1 - \frac{S}{|a_d|.|z|}\right) \geqslant |a_d|.|z| \left(1 - \frac{S}{|a_d|.|z|}\right).$$

  Ajoutons encore à z deux nouvelles contraintes : $|z| \geqslant \frac{2S}{|a_d|}$ et $|z| \geqslant \frac{2(m+1)}{|a_d|}$. Alors :

  $$\big|P(z)\big| \geqslant |a_d|.|z| \left(1 - \frac{1}{2}\right) = \frac{|a_d|.|z|}{2} \geqslant m + 1.$$

  Posons $K = \max\left\{1, \frac{2S}{|a_d|}, \frac{2(m+1)}{|a_d|}\right\}$. Conclusion : pour tout $z \in \mathbb{C}$ tel que $|z| \geqslant K$, $\big|P(z)\big| \geqslant m + 1$.

  Ce calcul un peu pénible ne fait qu'exprimer au fond l'idée que lorsque $|z|$ tend vers ∞, $\big|P(z)\big|$ tend vers ∞.

  3) Pour tout $n \in \mathbb{N}$: $\big|P(z_n)\big| < m + \frac{1}{2^n} \leqslant m+1$, donc par contraposition, d'après 2) : $|z_n| < K$, puis a fortiori : $\big|\mathrm{Re}(z_n)\big| \leqslant K$ et $\big|\mathrm{Im}(z_n)\big| \leqslant K$. Tout ça pour dire que les suites $\big(\mathrm{Re}(z_n)\big)_{n\in\mathbb{N}}$ et $\big(\mathrm{Im}(z_n)\big)_{n\in\mathbb{N}}$ sont bornées !

  Il s'agit ici d'extraire de la suite complexe **BORNÉE** $(z_n)_{n\in\mathbb{N}}$ une sous-suite convergente — théorème de Bolzano-Weierstrass pour les suites complexes.

  4) En vertu du théorème de Bolzano-Weierstrass, il existe une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante pour laquelle la suite $\big(\mathrm{Re}(z_{\varphi(n)})\big)_{n\in\mathbb{N}}$ converge, disons vers R. Appliquons une seconde fois le théorème de Bolzano-Weierstrass, cette fois à la suite $\big(\mathrm{Im}(z_{\varphi(n)})\big)_{n\in\mathbb{N}}$: il existe une application $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante pour laquelle la suite $\big(\mathrm{Im}(z_{\varphi\circ\psi(n)})\big)_{n\in\mathbb{N}}$ converge, disons vers I.
  Finalement : $\lim_{n\to\infty} \mathrm{Im}(z_{\varphi\circ\psi(n)}) = R$ et $\lim_{n\to\infty} \mathrm{Im}(z_{\varphi\circ\psi(n)}) = I$, donc $\lim_{n\to\infty} z_{\varphi\circ\psi(n)} = R + iI$.

  Par continuité de $|P|$, nous en déduisons que $\lim_{n\to\infty} \big|P(z_{\varphi\circ\psi(n)})\big| = \big|P(R+iI)\big|$. Mais rappelons que $\lim_{n\to\infty} \big|P(z_n)\big| = m$. Du coup $m = \big|P(R+iI)\big|$. C'est bien dire que m est un minimum de $|P|$ — pas seulement une borne inférieure. Posons $z_0 = R + iI$, point en lequel le minimum est atteint.

- Montrons que le minimum $m = \big|P(z_0)\big|$ de $|P|$ vaut forcément 0. Raisonnons pour cela par l'absurde en supposant $P(z_0) \neq 0$. Notons Q le polynôme $P(X + z_0)$ — par hypothèse, $Q(0) \neq 0$ — avec ses coefficients : $Q = b_0 + b_q X^q + b_{q+1} X^{q+1} + \ldots + b_d X^d$, où b_q est le premier coefficient non nul après $b_0 = Q(0) \neq 0$. Notons en outre θ un argument de $-\frac{b_0}{b_q}$, de sorte que $\frac{b_0}{b_q} = -\left|\frac{b_0}{b_q}\right| e^{i\theta}$. Fixons enfin $r \in]0, 1]$ et posons $z = re^{\frac{i\theta}{q}}$.

  $$\big|Q(z)\big| = \left|b_0 + b_q z^q + b_{q+1} z^{q+1} + \ldots + b_d z^d\right| \leqslant \big|b_0 + b_q z^q\big| + \sum_{k=q+1}^{d} |b_k|.|z|^k = |b_0|.\left|1 + \frac{b_q r^q e^{i\theta}}{b_0}\right| + \sum_{k=q+1}^{d} |b_k| r^k$$

  $$\overset{0<r\leqslant 1}{\leqslant} |b_0|.\left|1 - \left|\frac{b_q}{b_0}\right| r^q\right| + r^{q+1} \sum_{k=q+1}^{d} |b_k| = |b_0|.\left|1 - \left|\frac{b_q}{b_0}\right| r^q\right| + r^{q+1} T \qquad \text{si l'on pose } T = \sum_{k=q+1}^{d} |b_k| > 0.$$

  Choisissons a posteriori r inférieur ou égal à $\sqrt[q]{\left|\frac{b_0}{b_q}\right|}$ et $\frac{|b_q|}{2T}$. Alors : $1 - \left|\frac{b_q}{b_0}\right| r^q \geqslant 0$ et $r^{q+1} T \leqslant \frac{|b_q| r^q}{2}$,

  donc : $\big|Q(z)\big| \leqslant |b_0|.\left(1 - \left|\frac{b_q}{b_0}\right| r^q\right) + \frac{|b_q| r^q}{2} = |b_0| - \frac{|b_q| r^q}{2} < |b_0| = \big|Q(0)\big| = \big|P(z_0)\big| = m$.

  Finalement : $\big|P(z + z_0)\big| = \big|Q(z)\big| < m$. Cette inégalité stricte contredit le fait que m minore $|P|$. Ainsi comme voulu, $P(z_0) = 0$. ∎