Polynômes

Plan du chapitre

Dans tout ce chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

Dans ce chapitre (et dans nombre de chapitres ultérieurs), nous aurons besoin d'un nouvel objet, le symbole de Kronecker : pour $(i,j) \in \mathbb{N}^2$, on pose

$$\delta_{i,j} = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ si } i \neq j \end{cases}.$$

Ainsi, $\delta_{1,0} = 0$ et $\delta_{1,1} = 1$. Dans un premier temps, on ne voit pas bien l'utilité de ce symbole mais celui-ci s'avèrera très pratique à l'usage.

1 L'anneau $(\mathbb{K}[X], +, \times)$

1.1 Définition de $\mathbb{K}[X]$ et des opérations dans $\mathbb{K}[X]$

Comme le dit le programme officiel, « la construction de $\mathbb{K}[X]$ n'est pas exigible ». Nous vous en proposons une. En première lecture, vous pouvez sauter les démonstrations de ce paragraphe et ne vous concentrer que sur les résultats.

Définition 1. Un **polynôme à coefficients dans** $\mathbb{K}$ est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ qui est nulle à partir d'un certain rang.
Si $P = (a_n)_{n\in\mathbb{N}}$ est un polynôme, pour $n \in \mathbb{N}$, a_n est le **n-ème coefficient** du polynôme P.
On note X le polynôme $(0,1,0,0,0,\ldots) = (\delta_{n,1})_{n\in\mathbb{N}}$ et on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Un polynôme est donc la suite de ces coefficients, cette suite étant nulle à partir d'un certain rang. Ainsi défini, un polynôme n'a pas l'aspect qu'on lui connaît en terminale comme par exemple $2x^3 - x + 1$ (qui est la suite $(1,-1,0,2,0,0,0,\ldots)$). On va revenir assez rapidement à ce type de notation. Mais d'ores et déjà, avec cette présentation des polynômes, on peut immédiatement énoncer :

Théorème 1. Deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

On définit maintenant dans $\mathbb{K}[X]$ trois opérations : $+$, $.$ et $\times$.

Addition des polynômes. Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$ (les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont donc toutes deux nulles à partir d'un certain rang). On pose

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}}.$$

Multiplication des polynômes par un nombre. Soient $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On pose

$$\lambda.P = (\lambda a_n)_{n\in\mathbb{N}}.$$

Multiplication des polynômes. Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux éléments de $\mathbb{K}[X]$. On pose

$$P \times Q = (c_n)_{n\in\mathbb{N}} \text{ où } \forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{\substack{(i,j)\in[\![0,n]\!]^2 \\ i+j=n}} a_i b_j.$$

On a alors :

Théorème 2. $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Démonstration. (très longue et fastideuse.)

• Vérifions que $(\mathbb{K}[X], +)$ est un groupe commutatif.

- Vérifions que $+$ est une loi interne dans $\mathbb{K}[X]$. Soit $(P,Q) \in \mathbb{K}[X]^2$. Posons $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang. Par hypothèse, il existe $(n_1,n_2) \in \mathbb{N}^2$ tel que, pour $n \geqslant n_1$, $a_n = 0$ et pour $n \geqslant n_2$, $b_n = 0$.
Soit $n_0 = \text{Max}\{n_1,n_2\}$. n_0 est un entier naturel et pour $n \geqslant n_0$, $a_n = 0$ et $b_n = 0$ puis $a_n + b_n = 0$. Ceci montre que $P + Q$ est un élément de $\mathbb{K}[X]$.

On a montré que $+$ est une loi interne dans $\mathbb{K}[X]$.

- Vérifions que $+$ est commutative. Soit $(P,Q) \in \mathbb{K}[X]^2$. Posons $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang.

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}} = (b_n + a_n)_{n\in\mathbb{N}} = Q + P.$$

On a montré que $+$ est commutative.

- Vérifions que $+$ est associative. Soit $(P,Q,R) \in \mathbb{K}[X]^3$. Posons $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ et $R = (c_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$,

$(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang.

$$\begin{aligned}(P+Q)+R&=(a_n+b_n)_{n\in\mathbb{N}}+(c_n)_{n\in\mathbb{N}}=((a_n+b_n)+c_n)_{n\in\mathbb{N}}=(a_n+(b_n+c_n))_{n\in\mathbb{N}}=(a_n)_{n\in\mathbb{N}}+(b_n+c_n)_{n\in\mathbb{N}}\\&=P+(Q+R).\end{aligned}$$

On a montré que $+$ est associative (et on peut dorénavant écrire $P+Q+R$).

- Vérifions que $+$ possède un élément neutre. Posons $0=(0)_{n\in\mathbb{N}}$ (0 est un élément de $\mathbb{K}[X]$). Soit $P\in\mathbb{K}[X]$. Posons $P=(a_n)_{n\in\mathbb{N}}$ où la suite $(a_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang.

$$P+0=(a_n)_{n\in\mathbb{N}}+(0)_{n\in\mathbb{N}}=(a_n+0)_{n\in\mathbb{N}}=(a_n)_{n\in\mathbb{N}}=P.$$

Donc, $+$ possède un élément neutre, à savoir le polynôme noté 0 et appelé le **polynôme nul**.

- Vérifions que tout élément de $\mathbb{K}[X]$ possède un opposé (ou encore un symétrique pour $+$). Soit $P\in\mathbb{K}[X]$. Posons $P=(a_n)_{n\in\mathbb{N}}$ où la suite $(a_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang. Soit $Q=(-a_n)_{n\in\mathbb{N}}$. Q est un élément de $\mathbb{K}[X]$ et

$$P+Q=(a_n)_{n\in\mathbb{N}}+(-a_n)_{n\in\mathbb{N}}=(a_n+(-a_n))_{n\in\mathbb{N}}=(0)_{n\in\mathbb{N}}=0.$$

Donc, tout élément $P=(a_n)_{n\in\mathbb{N}}$ possède un opposé à savoir le polynôme, dorénavant noté $-P$, et égal à $(-a_n)_{n\in\mathbb{N}}$.

Ainsi, $(\mathbb{K}[X],+)$ est un groupe commutatif.

• Passons à la multiplication.

- Vérifions que $\times$ est une loi interne dans $\mathbb{K}[X]$. Soit $(P,Q)\in\mathbb{K}[X]^2$. Posons $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang. Par hypothèse, il existe $(n_1,n_2)\in\mathbb{N}^2$ tel que, pour $n\geqslant n_1$, $a_n=0$ et pour $n\geqslant n_2$, $b_n=0$. Posons encore $P\times Q=(c_n)_{n\in\mathbb{N}}=\left(\sum_{k=0}^{n}a_kb_{n-k}\right)_{n\in\mathbb{N}}$.

Soit $n_0=n_1+n_2$. Soit $n\geqslant n_0=n_1+n_2$. On a $c_n=\sum_{k=0}^{n}a_kb_{n-k}$. Dans cette somme, si $k\geqslant n_1$, alors $a_k=0$ puis $a_kb_{n-k}=0$.

Si $k<n_1$, alors $n-k>n-n_1\geqslant n_0-n_1=n_2$ et donc $b_{n-k}=0$ puis $a_kb_{n-k}=0$. Finalement, tous les termes de la somme sont nuls puis $c_n=0$. Ceci montre que $P\times Q\in\mathbb{K}[X]$.

On a montré que $\times$ est une loi interne dans $\mathbb{K}[X]$.

- Vérifions que $\times$ est commutative. Soit $(P,Q)\in\mathbb{K}[X]^2$. Posons $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang. En posant $l=n-k$, on obtient

$$P\times Q=\left(\sum_{k=0}^{n}a_kb_{n-k}\right)_{n\in\mathbb{N}}=\left(\sum_{l=0}^{n}b_la_{n-l}\right)_{n\in\mathbb{N}}=Q\times P.$$

Donc, $\times$ est commutative.

- Vérifions que $\times$ est associative. Soit $(P,Q,R)\in\mathbb{K}[X]^3$. Posons $P=(a_n)_{n\in\mathbb{N}}$, $Q=(b_n)_{n\in\mathbb{N}}$ et $R=(c_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang.

$$\begin{aligned}(P\times Q)\times R&=\left(\sum_{i=0}^{n}a_ib_{n-i}\right)_{n\in\mathbb{N}}\times(c_n)_{n\in\mathbb{N}}=\left(\sum_{\substack{(i,j)\in[\![0,n]\!]^2\\ i+j=n}}a_ib_j\right)_{n\in\mathbb{N}}\times(c_n)_{n\in\mathbb{N}}\\&=\left(\sum_{k=0}^{n}\left(\sum_{\substack{(i,j)\in[\![0,n]\!]^2\\ i+j=n-k}}a_ib_j\right)c_k\right)_{n\in\mathbb{N}}=\left(\sum_{k=0}^{n}\left(\sum_{\substack{(i,j)\in[\![0,n]\!]^2\\ i+j+k=n}}a_ib_jc_k\right)\right)_{n\in\mathbb{N}}\\&=\left(\sum_{\substack{(i,j,k)\in[\![0,n]\!]^3\\ i+j+k=n}}^{n}a_ib_jc_k\right)_{n\in\mathbb{N}}.\end{aligned}$$

Par symétrie des rôles, on a aussi

$$P\times(Q\times R)=(Q\times R)\times P=\left(\sum_{\substack{(i,j,k)\in[\![0,n]\!]^3\\ i+j+k=n}}^{n}a_ib_jc_k\right)_{n\in\mathbb{N}},$$

et donc, $(P\times Q)\times R=P\times(Q\times R)$.

On a montré que $\times$ est associative (et on peut dorénavant écrire $P\times Q\times R$).

- Vérifions que $\times$ possède un élément neutre. Posons $1 = (1, 0, 0, 0, \ldots) = (\delta_{n,0})_{n\in\mathbb{N}}$. Soit $P \in \mathbb{K}[X]$. Posons $P = (a_n)_{n\in\mathbb{N}}$ où la suite $(a_n)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang.

$$P \times 1 = (a_n)_{n\in\mathbb{N}} \times (\delta_{n,0})_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} a_k \delta_{0,n-k}\right)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} = P.$$

Donc, $\times$ possède un élément neutre, à savoir le polynôme noté 1 et égal à $(\delta_{n,0})_{n\in\mathbb{N}}$.

• Vérifions enfin que $\times$ est distributive sur $+$. Soit $(P, Q, R) \in \mathbb{K}[X]^3$. Posons $P = (a_n)_{n\in\mathbb{N}}$, $Q = (b_n)_{n\in\mathbb{N}}$ et $R = (c_n)_{n\in\mathbb{N}}$ où les suites $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ sont nulles à partir d'un certain rang.

$$\begin{aligned}(P+Q)\times R &= (a_n+b_n)_{n\in\mathbb{N}} \times (c_n)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n}(a_k+b_k)\,c_{n-k}\right)_{n\in\mathbb{N}} = \left(\sum_{k=0}^{n} a_k c_{n-k} + \sum_{k=0}^{n} b_k c_{n-k}\right)_{n\in\mathbb{N}}\\ &= \left(\sum_{k=0}^{n} a_k c_{n-k}\right)_{n\in\mathbb{N}} + \left(\sum_{k=0}^{n} b_k c_{n-k}\right)_{n\in\mathbb{N}} = P\times R + Q\times R.\end{aligned}$$

Ceci montre que $\times$ est distributive sur $+$.

On a montré que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

❑

Cette longue démonstration étant achevée, on va maintenant se diriger vers une notation définitive des polynômes (une notation de la forme $P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$) et abandonner la notation $P = (a_n)_{n\in\mathbb{N}}$. On rappelle que X est le polynôme $(0, 1, 0, 0, 0, \ldots) = (\delta_{n,1})_{n\in\mathbb{N}}$ (X n'est donc pas un nombre, X s'appelle parfois l'« indéterminée »).

Soit $P = (a_k)_{n\in\mathbb{N}}$ un polynôme. Supposons que pour tout $k > n$, on a $a_k = 0$, où n est un certain entier naturel. On peut déjà écrire

$$\begin{aligned}P &= (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = (a_0, 0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \ldots + (0, 0, \ldots, 0, a_n, 0, 0, 0, \ldots)\\ &= a_0(1, 0, 0, 0, \ldots) + a_1(0, 1, 0, 0, \ldots) + \ldots + a_n(0, 0, \ldots, 0, 1, 0, 0, 0, \ldots)\\ &= a_0\,(\delta_{k,0})_{k\in\mathbb{N}} + a_1\,(\delta_{k,1})_{k\in\mathbb{N}} + \ldots + a_n\,(\delta_{k,n})_{k\in\mathbb{N}} \quad (*).\end{aligned}$$

On va maintenant montrer par récurrence que $\forall k \in \mathbb{N}^*$, $X^k = (\delta_{m,k})_{m\in\mathbb{N}}$.

- Le résultat est vrai pour $k = 1$ par définition de X.
- Soit $k \geqslant 1$. Supposons que $X^k = (\delta_{m,k})_{m\in\mathbb{N}}$. Alors,

$$\begin{aligned}X^{k+1} &= X^k \times X = (\delta_{m,k})_{m\in\mathbb{N}} \times (\delta_{m,1})_{m\in\mathbb{N}} \text{ (par hypothèse de récurrence)}\\ &= \left(\sum_{i=0}^{m} \delta_{i,1}\delta_{m-i,k}\right)_{m\in\mathbb{N}} = (\delta_{m-1,k})_{m\in\mathbb{N}} \text{ (quand } i \neq 1,\ \delta_{i,1}\delta_{m-i,k} = 0)\\ &= (\delta_{m,k+1})_{m\in\mathbb{N}} \text{ (car } m-1 = k \Leftrightarrow m = k+1).\end{aligned}$$

Le résultat est démontré par récurrence.

Si on pose de plus, conventionnellement, $X^0 = 1$ (le polynôme) puis $a_0X^0 = a_0$ (cette fois-ci a_0 est un polynôme dit « constant » (on a donc identifié un élément de $\mathbb{K}$ et un polynôme constant)), l'égalité $(*)$ s'écrit alors

$$P = a_0 + a_1X + \ldots + a_nX^n = \sum_{k=0}^{n} a_kX^k.$$

Ainsi, tout élément P de $\mathbb{K}[X]$ peut s'écrire sous la forme : $P = \sum_{k=0}^{n} a_kX^k$ où $n \in \mathbb{N}$ et où $(a_0, a_1, \ldots, a_n) \in (\mathbb{K}[X])^{n+1}$.

n ne désigne pas nécessairement le degré de P (qui sera analysé au paragraphe suivant). n n'est le degré de P que si $a_n \neq 0$. Si les a_k sont nuls au delà d'un certain rang n (et peut-être avant) et si p est un entier supérieur ou égal à n, on peut écrire $P = \sum_{k=0}^{n} a_kX^k = \sum_{k=0}^{p} a_kX^k$.

On peut aussi écrire $P = \sum_{k=0}^{+\infty} a_kX^k$, cette dernière somme étant en fait finie.

Les différentes opérations peuvent se réécrire sous la forme :

- $P+Q=\sum_{k=0}^{+\infty}a_kX^k+\sum_{k=0}^{+\infty}b_kX^k=\sum_{k=0}^{+\infty}(a_k+b_k)X^k$.
- $\lambda P=\lambda\sum_{k=0}^{+\infty}a_kX^k=\sum_{k=0}^{+\infty}(\lambda a_k)X^k$.
- $P\times Q=\sum_{k=0}^{+\infty}a_kX^k\times\sum_{k=0}^{+\infty}b_kX^k=\sum_{k=0}^{+\infty}\left(\sum_{i=0}^{k}a_ib_{k-i}\right)X^k=\sum_{k=0}^{+\infty}\left(\sum_{\substack{(i,j)\in[\![0,k]\!]^2\\ i+j=k}}a_ib_j\right)X^k$.

Ainsi, le coefficient de X^2 dans le développement de $\left(3X^2-7X+1\right)\left(X^2+4X+5\right)$ est

$$a_2b_0+a_1b_1+a_0b_2=3\times5+(-7)\times4+1\times1=-12.$$

De manière plus complète, le développement de $\left(3X^2-7X+1\right)\left(X^2+4X+5\right)$ doit dorénavant être pensé correctement sous la forme

$$\begin{aligned}&\left(3X^2-7X+1\right)\left(X^2+4X+5\right)\\&\qquad=(3\times1)X^4+(3\times4+(-7)\times1)X^3+(3\times5+(-7)\times4+1\times1)X^2+((-7)\times5+1\times4)X+(1\times5)\\&\qquad=3X^4+5X^3-12X^2-31X+5\end{aligned}$$

et ne doit plus être pensé sous la forme

$$\begin{aligned}&\left(3X^2-7X+1\right)\left(X^2+4X+5\right)\\&\qquad=3X^4+12X^3+15X^2-7X^3-28X^2-35X+X^2+4X+5\\&\qquad=3X^4+5X^3-12X^2-31X+5.\end{aligned}$$

1.2 Degré d'un polynôme et coefficient dominant d'un polynôme non nul

1.2.1 Définition du degré et du coefficient dominant

Soit P un élément **non nul** de $\mathbb{K}[X]$. Soit $(a_k)_{n\in\mathbb{N}}$ la suite des coefficients de P. Soit $\mathcal{E}=\{k\in\mathbb{N}/\ a_k\neq0\}$.
Puisque P n'est pas le polynôme nul, l'ensemble $\mathcal{E}$ est une partie non vide de $\mathbb{N}$. D'autre part, par définition, la suite $(a_k)_{n\in\mathbb{N}}$ est nulle à partir d'un certain rang n_0. Donc, l'ensemble $\mathcal{E}$ est majoré (par n_0).
En résumé, $\mathcal{E}$ est une partie non vide et majorée de $\mathbb{N}$. On sait que $\mathcal{E}$ admet un plus grand élément. On peut donc poser :

Définition 2. Soient P un élément **non nul** de $\mathbb{K}[X]$ puis $(a_k)_{k\in\mathbb{N}}$ la suite de ses coefficients.

Le **degré** de P, noté $\deg(P)$ (ou $d^\circ(P)$), est

$$\deg(P)=\text{Max}\{k\in\mathbb{N}/\ a_k\neq0\}.$$

Si P est le polynôme nul, le degré de P est conventionnellement $-\infty$: $\deg(0)=-\infty$.

La convention adoptée sur le degré du polynôme nul trouvera entre autres sa justification avec la formule $\deg(P\times Q)=\deg(P)+\deg(Q)$, formule valable pour tous polynômes P et Q.

Notation. L'ensemble des polynômes à coefficients dans $\mathbb{K}$, de degré inférieur ou égal à n, se note $\mathbb{K}_n[X]$:

$$\mathbb{K}_n[X]=\left\{\sum_{k=0}^{n}a_kX^k,\ (a_0,\dots,a_n)\in\mathbb{K}^{n+1}\right\}.$$

Ainsi, $\mathbb{R}_2[X]=\left\{aX^2+bX+c,\ (a,b,c)\in\mathbb{R}^3\right\}$. Un élément aX^2+bX+c de $\mathbb{R}_2[X]$ est de degré 2 si $a\neq0$, de degré 1 si $a=0$ et $b\neq0$, de degré 0 si $a=b=0$ et $c\neq0$ et de degré $-\infty$ si $a=b=c=0$.
$\mathbb{K}_0[X]$ est l'ensemble des polynômes constants. Il est constitué des polynômes constants non nuls qui sont les polynômes de degré 0 et du polynôme nul qui est de degré $-\infty$.

DÉFINITION 3. Soient $P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$, un élément **non nul** de $\mathbb{K}[X]$, de degré $n \in \mathbb{N}$.

Le **coefficient dominant** de P, noté $\text{dom}(P)$, est : $\text{dom}(P) = a_n$.

Un polynôme non nul est **unitaire** (ou normalisé) si et seulement si son coefficient dominant est égal à 1.

1.2.2 Propriétés des degrés et des coefficients dominants

Dans ce paragraphe, on analyse le comportement du degré avec les différentes opérations déjà définies. On commence par l'addition.

Théorème 3. Pour tout $(P, Q) \in (\mathbb{K}[X])^2$, $\deg(P+Q) \leqslant \text{Max}\{\deg(P), \deg(Q)\}$.
De plus, si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \text{Max}\{\deg(P), \deg(Q)\}$.

DÉMONSTRATION. Si $P = 0$, alors $\deg(P) = -\infty$ puis $\text{Max}\{\deg(P), \deg(Q)\} = \deg(Q)$. D'autre part, $P + Q = Q$ et donc $\deg(P+Q) = \deg(Q)$. Dans ce cas, $\deg(P+Q) = \text{Max}\{\deg(P), \deg(Q)\} \leqslant \text{Max}\{\deg(P), \deg(Q)\}$. De même, si $Q = 0$.

Si $P \neq 0$ et $Q \neq 0$, on peut poser $n = \deg(P) \in \mathbb{N}$ et $p = \deg(Q) \in \mathbb{N}$. On note $(a_k)_{k\in\mathbb{N}}$ (resp. $(b_k)_{k\in\mathbb{N}}$) la suite des coefficients de P (resp. de Q).
Pour $k > \text{Max}\{n, p\}$, $a_k = 0$ et $b_k = 0$ puis $a_k + b_k = 0$. Donc, $\deg(P+Q) \leqslant \text{Max}\{n, p\} = \text{Max}\{\deg(P), \deg(Q)\}$.

Supposons de plus $\deg(P) \neq \deg(Q)$. Supposons par exemple $p < n$ de sorte que $\text{Max}\{\deg(P), \deg(Q)\} = n$. On sait déjà que si $k > n$, on a $a_k + b_k = 0$. Mais de plus, $a_n + b_n = a_n \neq 0$. Donc, $\deg(P+Q) = n = \text{Max}\{\deg(P), \deg(Q)\}$.

❑

Théorème 4. Pour tout $(\lambda, P) \in \mathbb{K} \times \mathbb{K}[X]$, $\deg(\lambda P) \leqslant \deg(P)$.
Plus précisément, si $\deg(\lambda P) = \begin{cases} \deg(P) \text{ si } \lambda \neq 0 \\ -\infty \text{ si } \lambda = 0 \end{cases} \leqslant \deg(P)$.

DÉMONSTRATION. Si $P = 0$, pour tout $\lambda \in \mathbb{K}$, $\deg(\lambda P) = -\infty = \deg(P) = \begin{cases} \deg(P) \text{ si } \lambda \neq 0 \\ -\infty \text{ si } \lambda = 0 \end{cases}$.

Sinon $P \neq 0$ et on peut poser $n = \deg(P) \in \mathbb{N}$. On note $(a_k)_{k\in\mathbb{N}}$ la suite des coefficients de P.
Si $\lambda = 0$, $\deg(\lambda P) = -\infty \leqslant \deg(P)$. Si maintenant $\lambda \neq 0$, pour $k > n$, on a $\lambda a_k = 0$ et donc, $\deg(\lambda P) \leqslant n = \deg(P)$. D'autre part, $\lambda a_n \neq 0$ et donc $\deg(\lambda P) = n = \deg(P)$.

❑

⇨ **Commentaire**.

◇ *On note au passage que si $\lambda \neq 0$ et $P \neq 0$, alors dom$(\lambda P) = \lambda$ dom(P).*

◇ *Si on combine les résultats des théorèmes 3 et 4, on obtient pour tout $(\lambda, \mu) \in \mathbb{K}^2$ et tout $(P, Q) \in (\mathbb{K}[X])^2$, deg$(\lambda P + \mu Q) \leqslant$ Max$\{$deg(P), deg$(Q)\}$.*

Théorème 5. • Pour tout $(P, Q) \in (\mathbb{K}[X])^2$, $\deg(P \times Q) = \deg(P) + \deg(Q)$
(avec les conventions usuelles : $\forall n \in \mathbb{N}$, $(-\infty) + n = -\infty$ et $(-\infty) + (-\infty) = -\infty$).

Si $P \neq 0$ et $Q \neq 0$, alors $\text{dom}(P \times Q) = \text{dom}(P) \times \text{dom}(Q)$.

• En particulier, $\forall n \in \mathbb{N}^*$, $\forall P \in \mathbb{K}[X]$, $\deg(P^n) = n \deg(P)$.

DÉMONSTRATION. Si $P = 0$, alors $P \times Q = 0$ puis $\deg(P \times Q) = -\infty = -\infty + \deg(Q) = \deg(P) + \deg(Q)$. De même, si $Q = 0$.

Si $P \neq 0$ et $Q \neq 0$, on peut poser $n = \deg(P) \in \mathbb{N}$ et $p = \deg(Q) \in \mathbb{N}$. On note $(a_k)_{k\in\mathbb{N}}$ (resp. $(b_k)_{k\in\mathbb{N}}$, $(c_k)_{k\in\mathbb{N}}$) la suite des coefficients de P (resp. de Q, de $P \times Q$).

Soit $k > n + p$ (et donc en particulier $k > n$). On a $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Dans cette somme, si $i > n$, alors $a_i = 0$ puis $a_i b_{k-i} = 0$ et si $i \leqslant n$, alors $k - i \geqslant k - n > n + p - n = p$ et donc $b_{k-i} = 0$ puis $a_i b_{k-i} = 0$. Ainsi, tous les termes de la somme égale à c_k sont nuls et donc $c_k = 0$. Ceci montre déjà que $\deg(P \times Q) \leqslant n + p = \deg(P) + \deg(Q)$.

Ensuite, $c_{n+p} = \sum_{i=0}^{n+p} a_i b_{n+p-i}$. Dans cette somme, si $i > n$, alors $a_i = 0$ puis $a_i b_{n+p-i} = 0$ et si $i < n$, alors $n + p - i > n + p - n = p$ et donc $b_{n+p-i} = 0$ puis $a_i b_{n+p-i} = 0$. Il ne reste que le terme numéro $i = n$: $c_{n+p} = a_n b_p \neq 0$.

Ceci montre que $\deg(P\times Q)=\deg(P)+\deg(Q)$. On note de plus que $\mathrm{dom}(P\times Q)=c_{n+p}=a_n\times b_p=\mathrm{dom}(P)\times\mathrm{dom}(Q)$.

L'égalité $\deg\left(P^n\right)=n\deg(P)$ s'en déduit par récurrence.

❑

⇨ **Commentaire**. *On va voir à l'usage que la formule sur le degré d'un produit est la seule formule sur les degrés « qui se passe bien ». Toutes les autres formules (d'autres formules sont à venir) comportent des conditions de validité. Par exemple le degré de* (λP) *n'est pas le degré de* P *mais est le degré de* P *si* $\lambda\neq 0$ *et est* $-\infty$ *si* $\lambda=0$.

Exercice 1. Pour $n\geqslant 2$, on pose $P_n=(X+1)^n-(X-1)^n$.

Déterminer le degré de P_n et son coefficient dominant.

Solution 1. $\deg\left((X+1)^n\right)=n$ et $\deg\left((X-1)^n\right)=n$. Donc, $\deg\left(P_n\right)\leqslant n$. Plus précisément, d'après la formule du binôme de Newton, il existe deux polynômes Q_1 et Q_2 de degrés au plus $n-2$ tels que

$$\begin{aligned}P_n&=(X+1)^n-(X-1)^n=\left(X^n+nX^{n-1}+Q_1\right)-\left(X^n-nX^{n-1}+Q_2\right)\\&=2nX^{n-1}+Q_1-Q_2.\end{aligned}$$

Puisque $\deg\left(Q_1-Q_2\right)\leqslant \mathrm{Max}\{\deg\left(Q_1\right),\deg\left(Q_2\right)\}\leqslant n-2$, on en déduit que

$$\deg\left(P_n\right)=\deg\left(2nX^{n-1}\right)=n-1$$

et

$$\mathrm{dom}\left(P_n\right)=\mathrm{dom}\left(2nX^{n-1}\right)=2n.$$

Si P est un polynôme donné, on peut définir une autre notion qui n'est pas, à proprement parler, au programme de maths sup et de maths spé : la notion de **valuation** du polynôme P, notée $\mathrm{val}(P)$.

Si $P=\sum_{k=0}^{+\infty}a_kX^k$ est un polynôme non nul, $\mathrm{val}(P)=\mathrm{Min}\{k\in\mathbb{N}/\ a_k\neq 0\}$ et si $P=0$, conventionnellement $\mathrm{val}(P)=+\infty$.

Par exemple, $\mathrm{val}\left(X^5-X^3+X^2+1\right)=0$ et $\deg\left(X^5-X^3+X^2+1\right)=5$ ou aussi $\mathrm{val}\left(X^5+2X^3+X^2\right)=2$ et $\deg\left(X^5+2X^3+X^2\right)=5$ ou enfin $\mathrm{val}(0)=+\infty$ et $\deg(0)=-\infty$.

On peut montrer que la valuation a des propriétés de calculs analogues aux propriétés de calcul des degrés :

- $\mathrm{val}(P+Q)\geqslant\mathrm{Min}\{\mathrm{val}(P),\mathrm{val}(Q)\}$ et si de plus, $\mathrm{val}(P)\neq\mathrm{val}(Q)$, alors $\mathrm{val}(P+Q)=\mathrm{Min}\{\mathrm{val}(P),\mathrm{val}(Q)\}$.
- $\mathrm{val}(\lambda P)\geqslant\mathrm{val}(P)$ et si de plus, $\lambda\neq 0$, alors $\mathrm{val}(\lambda P)=\mathrm{val}(P)$.
- $\mathrm{val}(P\times Q)=\mathrm{val}(P)+\mathrm{val}(Q)$.

1.3 Intégrité de l'anneau $(\mathbb{K}[X],+,\times)$

Théorème 6. Dans l'anneau $(\mathbb{K}[X],+,\times)$, un produit de facteurs est nul si et seulement si l'un de ses facteurs est nuls (on dit alors que l'anneau commutatif $(\mathbb{K}[X],+,\times)$ est **intègre**).

Dit autrement, $\forall(P,Q)\in(\mathbb{K}[X])^2,\ (P\times Q=0\Rightarrow P=0\text{ ou }Q=0)$ (l'implication $\Leftarrow$ étant automatiquement vraie).

Démonstration. Soit $(P,Q)\in(\mathbb{K}[X])^2$. Si $P\neq 0$ et $Q\neq 0$, les polynômes P et Q ont des degrés éléments de $\mathbb{N}$. Mais alors $\deg(P\times Q)=\deg(P)+\deg(Q)\in\mathbb{N}$. En particulier, $P\times Q\neq 0$.
En résumé, $(P\neq 0\text{ et }Q\neq 0\Rightarrow P\times Q\neq 0)$. Par contraposition, $(P\times Q=0\Rightarrow P=0\text{ ou }Q=0)$.

❑

On déduit du théorème précédent les polynômes qui sont simplifiables pour la multiplication : ce sont les polynômes non nuls.

Théorème 7. $\forall(P,Q,R)\in(\mathbb{K}[X])^3,\ (P\times Q=P\times R\text{ et }P\neq 0\Rightarrow Q=R)$.

Démonstration. Soit $(P,Q,R)\in(\mathbb{K}[X])^3$ tel que $P\neq 0$. Par intégrité de l'anneau $(\mathbb{K}[X],+,\times)$,

$$PQ=PR\Rightarrow P(Q-R)=0\Rightarrow Q-R=0\Rightarrow Q=R.$$

❑

Ainsi, par exemple, $(X-1)P=0 \Rightarrow P=0$ ou $(X-1)P=(X-1)Q \Rightarrow P=Q$ car $X-1$ n'est pas le polynôme nul. Il n'est par contre, pas question de justifier les implications précédentes par une phrase du genre « Pour $X \neq 1$, ... » car X **est différent de** 1 (X n'est pas un nombre mais X est un polynôme et le polynôme X n'est pas le polynôme 1).

1.4 Inversibles de l'anneau $(\mathbb{K}[X],+,\times)$

On s'intéresse maintenant aux polynômes P « tels que $\frac{1}{P}$ soit aussi un polynôme ».

Théorème 8. Les inversibles de l'anneau $(\mathbb{K}[X],+,\times)$ sont les constantes non nulles.

Démonstration. Soit $P \in \mathbb{K}[X]$. On suppose que P est inversible. Donc, il existe un polynôme Q tel que $P \times Q = 1$. Ceci impose déjà $P \neq 0$ et $Q \neq 0$ (d'après le théorème 6) et donc P et Q ont des degrés qui sont des entiers naturels. Ensuite,

$$P \times Q = 1 \Rightarrow \deg(P \times Q) = \deg(1) \Rightarrow \deg(P) + \deg(Q) = 0.$$

Si $\deg(P) \geqslant 1$, alors $\deg(P) + \deg(Q) \geqslant \deg(P) \geqslant 1 > 0$ ce qui est faux. Donc, nécessairement, $\deg(P) = 0$ ou encore, P est une constante non nulle.

Réciproquement, si $P = a_0 \neq 0$ (« $P \in \mathbb{K} \setminus \{0\}$ » ou plutôt $P \in \mathbb{K}_0[X] \setminus \{0\}$), alors, si $Q = \frac{1}{a_0} \in \mathbb{K}[X]$, on a $P \times Q = 1$ et donc P est inversible dans l'anneau $(\mathbb{K}[X],+\times)$.

❑

On note que les polynômes de degré au moins égal à 1 ne sont pas inversibles (pour $\times$) mais sont tout de même simplifiables (pour $\times$). Les deux notions (inversibles et simplifiables) ne sont donc pas équivalentes.

1.5 Composition des polynômes

Définition 4. Soient $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul, de degré $n \in \mathbb{N}$, et Q un polynôme non nul.

On pose $P \circ Q = \sum_{k=0}^{n} a_k Q^k$ avec la convention $Q^0 = 1$.

⇨ **Commentaire.** *Si on adopte la convention douteuse que l'égalité* $Q^0 = 1$ *est vraie y compris quand* $Q = 0$*, alors la définition de* $P \circ Q$ *reste valable quand* $P = 0$ *et/ou* $Q = 0$*.*

Exemple. Si $P = X^3 - 2X^2 + 1$, le polynôme $P \circ X^2$, plus simplement noté $P\left(X^2\right)$, est le polynôme :

$$P\left(X^2\right) = \left(X^2\right)^3 - 2\left(X^2\right)^2 + 1 = X^6 - 2X^4 + 1$$

et le polynôme $P \circ (X+1)$, plus simplement noté $P(X+1)$, est le polynôme

$$P(X+1) = (X+1)^3 - 2(X+1)^2 + 1 = X^3 + X^2 - X.$$

Si $P = (X+1)^2 - 4$, on peut démontrer (et nous l'admettrons sans rajouter de théorèmes et démonstrations supplémentaires) que $P\left(X^2\right) = \left(X^2+1\right)^2 - 4$ en remplaçant mécaniquement X par X^2 dans l'expression de P, sans avoir besoin de développer et réduire d'abord l'expression de P.

Théorème 9. Soit $(P,Q) \in (\mathbb{K}[X] \setminus \{0\})^2$. Alors, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Démonstration. Le résultat est clair si $\deg(P) = 0$ (dans ce cas, $P \circ Q$ est un polynôme constant non nul).

Posons $P = \sum_{k=0}^{n} a_k X^k$, $n \in \mathbb{N}^*$, $a_n \neq 0$ (de sorte que $n = \deg(P)$) et $Q = \sum_{k=0}^{p} b_k X^k$, $p \in \mathbb{N}$, $b_p \neq 0$ (de sorte que $p = \deg(Q)$).

$P \circ Q = \sum_{k=0}^{n} a_k Q^k = \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{p} b_i X^i\right)^k$. D'après le théorème 5, $\forall k \in [\![0,n]\!]$, $\deg\left(Q^k\right) = k \deg(Q) = kp$. On en déduit encore, d'après les théorèmes 3 et 4, que $\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right) \leqslant p(n-1)$. D'autre part, puisque $a_n \neq 0$, $\deg\left(a_n Q^n\right) = \deg\left(Q^n\right) = np$. Puisque

$\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right) < \deg(a_n Q^n)$, d'après le théorème 3

$$\deg(P \circ Q) = \deg(a_n Q^n) = \deg(Q^n) = np = \deg(P) \times \deg(Q).$$

❑

Ainsi, si P est un polynôme non nul, $\deg\left(P\left(X^2\right)\right) = 2\deg(P)$ et $\deg(P(X+1)) = \deg(P)$.

1.6 Dérivation formelle des polynômes

Depuis le début du chapitre, nous nous occupons de l'**aspect formel** des polynômes c'est-à-dire de tout ce qui concerne les **coefficients** de ces polynômes.

Il existe un autre aspect des polynômes : l'aspect **fonctionnel** (quand on évalue un polynôme en un nombre : $\forall x \in \mathbb{R}$, $P(x) = \ldots$). L'aspect fonctionnel des polynômes sera analysé à partir de la section 3 « Fonctions polynômes »).

Nous allons maintenant définir la **dérivée formelle** d'un polynôme : cette dérivée sera définie à partir des coefficients et pas du tout comme la limite quand x tend vers x_0 de $\dfrac{P(x) - P(x_0)}{x - x_0}$. Cette définition tient bien sûr compte de l'allure générale de la dérivée d'une fonction polynôme que l'on connaît depuis la classe de première.

Pourquoi tant de complications ? Parce que, à plus haut niveau, on peut définir la notion de polynôme sur un corps $\mathbb{K}$ quelconque (en maths sup, nous ne connaissons que très peu d'exemples de corps à part $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ (ou $\mathbb{Q}$)), corps $\mathbb{K}$ dans lesquels la notion de limite n'a plus aucun sens. Le premier exemple d'un tel corps apparaît en maths spé.

1.6.1 Dérivée première

DÉFINITION 5. Soit $P \in \mathbb{K}[X]$. On définit le **polynôme dérivé** du polynôme P, noté P', de la manière suivante :

Si $\deg(P) \leqslant 0$, on pose $P' = 0$.

Si $n = \deg(P) \geqslant 1$ et si $P = \sum_{k=0}^{n} a_k X^k$, on pose $P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$.

Par exemple, la dérivée du polynôme $P = 4X^3 - 7X^2 + X + 1$ est $P' = 12X^2 - 14X + 1$.

De manière générale, l'écriture $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ est la plus naturelle mais pas forcément la meilleure, parce que le terme général est mal décrit : X^{k-1} et pas X^k. On doit aussi prendre garde au démarrage de la somme ($k = 1$ et pas $k = 0$). Quand $k = 0$, le terme $k a_k X^{k-1}$ s'écrit plus explicitement $0 \times a_0 \times \dfrac{1}{X}$ et on ne voit pas très bien ce que viendrait faire $\dfrac{1}{X}$ dans la dérivée d'un polynôme. Ce sera encore pire en évaluant en un nombre x : $\dfrac{1}{x}$ n'a pas de sens quand $x = 0$.

On a immédiatement

Théorème 10.

Pour tout $P \in \mathbb{K}[X]$, $\deg(P') = \begin{cases} -\infty \text{ si } \deg(P) \leqslant 0 \\ \deg(P) - 1 \text{ si } \deg(P) \geqslant 1 \end{cases}$ puis, si $n = \deg(P) \geqslant 1$, $\operatorname{dom}(P') = n \operatorname{dom}(P)$.

On donne maintenant les différentes formules de dérivation formelle. Le théorème qui suit est immédiat (y compris dans les cas où P ou Q est constant).

Théorème 11.

1) $\forall (P, Q) \in (\mathbb{K}[X])^2$, $(P+Q)' = P' + Q'$.
2) $\forall (\lambda, P) \in \mathbb{K} \times \mathbb{K}[X]$, $(\lambda P)' = \lambda P'$.
3) $\forall (P, Q) \in (\mathbb{K}[X])^2$, $\forall (\lambda, \mu) \in \mathbb{K}^2$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.

Théorème 12.

1) $\forall (P,Q) \in (\mathbb{K}[X])^2$, $(P \times Q)' = P'Q + PQ'$.
2) $\forall P \in \mathbb{K}[X]$, $\forall n \in \mathbb{N}^*$, $(P^n)' = nP'P^{n-1}$.

3) $\forall n \geqslant 2$, $\forall (P_1, \dots, P_n) \in (\mathbb{K}[X])^n$, $(P_1 \times \dots \times P_n)' = \sum_{i=1}^{n} \left(P_i' \prod_{j \neq i} P_j \right)$.

Démonstration .

1) Le résultat est clair si $\deg(P) \leqslant 0$ ou $\deg(Q) \leqslant 0$.

Dorénavant, $\deg(P) \geqslant 1$ et $\deg(Q) \geqslant 1$. Posons $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ (le plus pratique pour manipuler les sommes qui suivent) où les suites $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont nulles à partir d'un certain rang.

$$\begin{aligned}
P'Q + PQ' &= \left(\sum_{n=0}^{+\infty} (n+1)a_{n+1}X^n\right)\left(\sum_{n=0}^{+\infty} b_n X^n\right) + \left(\sum_{n=0}^{+\infty} a_n X^n\right)\left(\sum_{n=0}^{+\infty} (n+1)b_{n+1}X^n\right) \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k}\right)X^n + \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} a_k(n-k+1)b_{n-k+1}\right)X^n \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k} + \sum_{k=0}^{n}(n-k+1)a_k b_{n+1-k}\right)X^n \\
&= \sum_{n=0}^{+\infty}\left(\sum_{l=1}^{n+1} l a_l b_{n-(l-1)} + \sum_{k=0}^{n}(n-k+1)a_k b_{n+1-k}\right)X^n \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=1}^{n+1} k a_k b_{n+1-k} + \sum_{k=0}^{n}(n-k+1)a_k b_{n+1-k}\right)X^n \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n+1} k a_k b_{n+1-k} + \sum_{k=0}^{n+1}(n-k+1)a_k b_{n+1-k}\right)X^n \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n+1}(k+n-k+1)a_k b_{n+1-k}\right)X^n = \sum_{n=0}^{+\infty}(n+1)\left(\sum_{k=0}^{n+1} a_k b_{n+1-k}\right)X^n \\
&= \sum_{n=0}^{+\infty} n\left(\sum_{k=0}^{n} a_k b_{n-k}\right)X^{n-1} = (P\times Q)'.
\end{aligned}$$

2) Le cas $n = 2$ est le cas $Q = P$ dans 1) : $\left(P^2\right)' = P'P + PP' = 2P'P$ et si, pour $n \geqslant 2$, $(P^n)' = nP'P^{n-1}$, alors

$$\left(P^{n+1}\right)' = (P^n \times P)' = (P^n)'P + P^n P' = nP'P^{n-1} \times P + P'P^n = nP'P^n + P'P^n = (n+1)P'P^n.$$

Le résultat est démontré par récurrence.

3) Le cas $n = 2$ est 1) et si, pour $n \geqslant 2$, $(P_1 \dots P_n)' = \sum_{i=1}^{n}\left(P_i' \prod_{\substack{1\leqslant j\leqslant n \\ j\neq i}} P_j\right)$, alors

$$\begin{aligned}
(P_1 \dots P_n P_{n+1})' &= (P_1 \dots P_n)' P_{n+1} + P_1 \dots P_n P_{n+1}' \\
&= \left(\sum_{i=1}^{n}\left(P_i' \prod_{\substack{1\leqslant j\leqslant n \\ j\neq i}} P_j\right)\right) P_{n+1} + P_1 \dots P_n P_{n+1}' \text{ (par hypothèse de récurrence)} \\
&= \left(\sum_{i=1}^{n}\left(P_i' \prod_{\substack{1\leqslant j\leqslant n+1 \\ j\neq i}} P_j\right)\right) + P_1 \dots P_n P_{n+1}' = \sum_{i=1}^{n+1} P_i' \left(\prod_{\substack{1\leqslant j\leqslant n+1 \\ j\neq i}} P_j\right).
\end{aligned}$$

Le résultat est démontré par récurrence.

❑

On peut démontrer aussi (mais nous ne le ferons pas) que

Théorème 13. $\forall (P,Q) \in (\mathbb{K}[X]\setminus\{0\})^2$,

$$(P\circ Q)' = (P'\circ Q)\times Q'.$$

1.6.2 Dérivées successives

DÉFINITION 6. Soit $P \in \mathbb{K}[X]$. On définit par récurrence la **dérivée k-ème** de P, notée $P^{(k)}$, par :

$$P^{(0)} = P \text{ et } \forall k \in \mathbb{N},\ P^{(k+1)} = \left(P^{(k)}\right)'$$

Analysons les dérivées successives du monôme X^n. Si $n \geqslant 1$, $(X^n)' = nX^{n-1}$. Si $n \geqslant 2$, $(X^n)'' = n(n-1)X^{n-2}$. Plus généralement, si $n \geqslant p \geqslant 1$,

$$(X^n)^{(p)} = n(n-1)\dots(n-p+1)X^{n-p} = \frac{n(n-1)\dots(n-p+1)(n-p)\dots 1}{(n-p)\dots 1}X^{n-p} = \frac{n!}{(n-p)!}X^{n-p}.$$

Cette dernière égalité reste vraie quand $p = 0$. D'autre part, si $p > n$, $(X^n)^{(p)} = 0$. On peut donc énoncer :

Théorème 14.

1) $\forall (n,p) \in \mathbb{N}$, si $p \leqslant n$,

$$(X^n)^{(p)} = \frac{n!}{(n-p)!}X^{n-p}$$

et si $p > n$, $(X^n)^{(p)} = 0$.

2) $\forall P = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$, si $p \leqslant n$,

$$P^{(p)} = \sum_{k=p}^{n} \frac{k!}{(k-p)!}a_k X^{k-p} = \sum_{k=0}^{n-p} \frac{(k+p)!}{k!}a_{k+p}X^k$$

et si $p > n$, $P^{(p)} = 0$.

On note que la dérivée n-ème d'un polynôme de degré n n'est pas nulle mais est un polynôme de degré $n-n=0$ ou encore, si $\deg(P) = n \in \mathbb{N}$, $P^{(n)}$ est une constante non nulle à savoir $P^{(n)} = n!\mathrm{dom}(P)$. Pour obtenir le polynôme nul, il faut dériver **au moins une fois de plus** que le degré. Plus généralement, on a immédiatement

Théorème 15. Soit $P \in \mathbb{K}[X]\setminus\{0\}$. Posons $n = \deg(P) \in \mathbb{N}$. Alors

$$\forall k \in \mathbb{N},\ \deg\left(P^{(k)}\right) = \begin{cases} n-k \text{ si } k \leqslant n \\ -\infty \text{ si } k > n \end{cases}.$$

Exercice 2. Déterminer tous les polynômes $P \in \mathbb{R}[X]$ vérifiant $P(2X) = P'P''$.

Solution 2. Soit $P \in \mathbb{R}[X]$.

Si $\deg(P) \leqslant 1$ et $P(2X) = P'P''$, alors nécessairement $P = P'\left(\frac{X}{2}\right)P''\left(\frac{X}{2}\right) = 0$. Réciproquement, si $P = 0$, alors P est solution du problème.

Dorénavant, $n = \deg(P) \geqslant 2$. Alors, nécessairement

$$n = \deg(P(2X)) = \deg(P'P'') = \deg(P') + \deg(P'') = n-1+n-2 = 2n-3$$

puis $n = 3$. Posons alors $P = aX^3 + bX^2 + cX + d$ où $(a,b,c,d) \in \mathbb{R}^4$ et $a \neq 0$.

$$P(2X) = P'P'' \Leftrightarrow 8aX^3 + 4bX^2 + 2cX + d = \left(3aX^2 + 2bX + c\right)(6aX + 2b)$$
$$\Leftrightarrow 8aX^3 + 4bX^2 + 2cX + d = 18a^2X^3 + 18abX^2 + \left(4b^2 + 6ac\right)X + 2bc$$
$$\Leftrightarrow \left\{\begin{array}{l} 8a = 18a^2 \\ 4b = 18ab \\ 2c = 4b^2 + 6ac \\ d = 2bc \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} a = \dfrac{4}{9} \text{ (car } a \neq 0) \\ 4b = 8b \\ 2c = 4b^2 + \dfrac{8}{3}c \\ d = 2bc \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} a = \dfrac{4}{9} \\ b = 0 \\ c = 0 \\ d = 0 \end{array}\right. \Leftrightarrow P = \frac{4}{9}X^3.$$

Les polynômes solutions sont 0 et $\dfrac{4}{9}X^3$.

⇨ **Commentaire** .

◇ *L'exercice 2 est un premier exemple de résolution d'une équation où l'inconnue est un polynôme. On ne se lance quasiment jamais en cherchant le polynôme P sous la forme $P = \sum_{k=0}^{n} a_k X^k$ ou $P = \sum_{k=0}^{+\infty} a_k X^k$. On « débroussaille d'abord le terrain » en recherchant au préalable un certain nombre de propriétés imposées à un polynôme solution. Parmi ces propriétés, il y a le degré.*

◇ *Dans la solution, un moment important est l'**identification des coefficients** : $8a = 18a^2$, $4b = 18ab$ ... On rappelle que deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients. Par contre, une **catastrophe** aurait été : $8aX^3+4bX^2+2cX+d = 18a^2X^3 + 18abX^2 + \left(4b^2 + 6ac\right)X + 2bc \Leftrightarrow 8aX^3 = 18a^2X^3$ et $4bX^2 = 18abX^2$ ... car l'égalité de deux sommes : $A + B = C + D$ n'entraine en aucune façon $A = C$ et $B = D$. Par exemple, $1 + 3 = 2 + 2$ avec $1 \neq 3$ et $2 \neq 2$.*

Immédiatement, on a

Théorème 16. $\forall (P, Q) \in (\mathbb{K}[X])^2$, $\forall k \in \mathbb{N}$, $(\lambda P + \mu Q)^{(k)} = \lambda P^{(k)} + \mu Q^{(k)}$.

Ensuite,

Théorème 17 (formule de Leibniz). $\forall (P, Q) \in (\mathbb{K}[X])^2$, $\forall n \in \mathbb{N}$,

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

Démonstration . Soit $(P, Q) \in (\mathbb{K}[X])^2$. Montrons par récurrence que $\forall n \in \mathbb{N}$, $(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

- $(P \times Q)^{(0)} = P \times Q = P^{(0)} \times Q^{(0)}$. La formule à démontrer est vraie quand $n = 0$.
- Soit $n \geqslant 0$. Supposons que $(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

$$(P \times Q)^{(n+1)} = \left((P \times Q)^{(n)}\right)' = \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k)} Q^{(n-k)}\right)' \text{ (par hypothèse de récurrence)}$$
$$= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n-k+1)}\right) = \sum_{k=0}^{n} \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)}$$
$$= \sum_{l=1}^{n+1} \binom{n}{l-1} P^{(l)} Q^{(n-(l-1))} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} \text{ (en posant } l = k+1)$$
$$= \sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)} = P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) P^{(k)} Q^{(n+1-k)} + P^{(0)} Q^{(n+1)}$$
$$= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)}.$$

On a montré par récurrence que : $\forall n \in \mathbb{N}$, $(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$. ❑

Exercice 3. Pour $n \geqslant 2$, calculer la dérivée n-ème de $\left(X^2+3X+2\right)(X-1)^n$.

Solution 3.

1ère solution. Soit $n \geqslant 2$. D'après la formule de Leibniz

$$\begin{aligned}
\left(\left(X^2+3X+2\right)(X-1)^n\right)^{(n)} &= \sum_{k=0}^{n} \binom{n}{k} \left(X^2+3X+2\right)^{(k)} \left((X-1)^n\right)^{(n-k)} \\
&= \sum_{k=0}^{2} \binom{n}{k} \left(X^2+3X+2\right)^{(k)} \left((X-1)^n\right)^{(n-k)} \text{ (car, pour } k \geqslant 3,\ \left(X^2+3X+2\right)^{(k)} = 0) \\
&= \left(X^2+3X+2\right)^{(0)} \left((X-1)^n\right)^{(n)} + n\left(X^2+3X+2\right)' \left((X-1)^n\right)^{(n-1)} \\
&+ \frac{n(n-1)}{2}\left(X^2+3X+2\right)'' \left((X-1)^n\right)^{(n-2)} \\
&= \left(X^2+3X+2\right) \times n! + n(2X+3) \times \frac{n!}{1!}(X-1) + \frac{n(n-1)}{2} \times 2 \times \frac{n!}{2!}(X-1)^2 \\
&= n!\left(X^2+3X+2+n(2X+3)(X-1)+\frac{n(n-1)}{2}(X-1)^2\right) \\
&= \frac{n!}{2}\left(2\left(X^2+3X+2\right)+2n\left(2X^2+X-3\right)+n(n-1)\left(X^2-2X+1\right)\right) \\
&= \frac{n!}{2}\left(\left(n^2+3n+2\right)X^2+\left(-2n^2+4n+6\right)X+n^2-7n+4\right)
\end{aligned}$$

2ème solution. La formule du binôme de Newton fournit

$$\begin{aligned}
\left(X^2+3X+2\right)(X-1)^n &= \left(X^2+3X+2\right)\left(X^n-nX^{n-1}+\frac{n(n-1)}{2}X^{n-2}+\ldots\right) \\
&= X^{n+2}-(n-3)X^{n+1}+\left(\frac{n(n-1)}{2}-3n+2\right)X^n+\ldots \\
&= X^{n+2}-(n-3)X^{n+1}+\frac{n^2-7n+4}{2}X^n+\ldots
\end{aligned}$$

puis

$$\begin{aligned}
\left(\left(X^2+3X+2\right)(X-1)^n\right)^{(n)} &= \left(X^{n+2}-(n-3)X^{n+1}+\frac{n^2-7n+4}{2}X^n\right)^{(n)} \\
&= \frac{(n+2)!}{2!}X^2-(n-3)\frac{(n+1)!}{1!}X+\frac{n^2-7n+4}{2}n! \\
&= \frac{n!}{2}\left(\left(n^2+3n+2\right)X^2+\left(-2n^2+4n+6\right)X+n^2-7n+4\right).
\end{aligned}$$

---

2 Arithmétique dans $\mathbb{K}[X]$

On va constater que tout le cours d'arithmétique dans $\mathbb{Z}$ peut être reproduit quasiment à l'identique dans l'anneau $(\mathbb{K}[X],+,\times)$. Tout commence avec la division euclidienne dans $\mathbb{K}[X]$.

2.1 Division euclidienne dans $\mathbb{K}[X]$

Théorème 18 (division euclidienne dans $\mathbb{K}[X]$). Soit $(A,B) \in \mathbb{K}[X] \times (\mathbb{K}[X]\setminus\{0\})$. Il existe un couple $(Q,R) \in \mathbb{K}[X]^2$ et un seul tel que

$$A = B \times Q + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Démonstration .

Existence. On note que $\deg(B) \neq -\infty$ car $B \neq 0$. Posons $m = \deg(B) \in \mathbb{N}$ puis $B = \sum_{k=0}^{m} b_k X^k$ avec $b_m \neq 0$.

Si $\deg(A) < m$, on pose $Q = 0$ et $R = A$. On obtient $A = B \times Q + R$ avec $\deg(R) < \deg(B)$.

Si $m = 0$ (B est une constante non nulle), posons $B = b_0$. Alors, $A = QB + R$ où $Q = \dfrac{1}{b_0}A$ et $R = 0$ de sorte que $\deg(R) < \deg(B)$.
Dorénavant, on suppose que $m \geqslant 1$.

Montrons par récurrence que : $\forall n \geqslant m$, si $\deg(A) \leqslant n$, alors $\exists (Q,R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

- Soit A un polynôme de degré m (le cas où $\deg(A) < m$ a été analysé avant). Posons $A = \sum_{k=0}^{m} a_k X^k$ puis $Q = \dfrac{a_m}{b_m}$ (Q est un polynôme de degré 0) et $R = A - BQ$. Alors, R est un polynôme tel que $A = BQ + R$ et de plus,

$$R = \sum_{k=0}^{m} a_k X^k - \frac{a_m}{b_m} \sum_{k=0}^{m} b_k X^k = \sum_{k=0}^{m} \left(a_k - \frac{a_m}{b_m} b_k \right) X^k = \sum_{k=0}^{m-1} \left(a_k - \frac{a_m}{b_m} b_k \right) X^k,$$

et donc $\deg(R) < m$. L'affirmation est donc vraie quand $n = m$.

- Soit $n \geqslant m$. Supposons que pour tout polynôme A de degré inférieur ou égal à n, il existe $(Q,R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

Soit A un polynôme de degré $n+1$. Posons $A = \sum_{k=0}^{n+1} a_k X^k$. On peut déjà écrire

$$\begin{aligned} A - \frac{a_{n+1}}{b_m} X^{n+1-m} B &= \sum_{k=0}^{n+1} a_k X^k - \frac{a_{n+1}}{b_m} X^{n+1-m} \sum_{k=0}^{m} b_k X^k \\ &= a_{n+1} X^{n+1} + \sum_{k=0}^{n} a_k X^k - \frac{a_{n+1}}{b_m} \times b_m X^{n+1} + \sum_{k=0}^{m-1} \frac{a_{n+1}}{b_m} b_k X^{n+1-m+k} \\ &= \sum_{k=0}^{n} a_k X^k - \sum_{k=n+1-m}^{n} \frac{a_{n+1}}{b_m} b_{n+1-m+k} X^k. \end{aligned}$$

Par suite, $\deg\left(A - \dfrac{a_{n+1}}{b_m} X^{n+1-m} B \right) \leqslant n$. Par hypothèse de récurrence, il existe $(Q_1, R) \in \mathbb{K}[X]^2$ tel que $A - \dfrac{a_{n+1}}{b_m} X^{n+1-m} B = BQ_1 + R$ et $\deg(R) < \deg(B)$. Mais alors,

$$A = B\left(\frac{a_{n+1}}{b_m} X^{n+1-m} + Q_1 \right) + R$$

et les polynômes $Q = \dfrac{a_{n+1}}{b_m} X^{n+1-m} + Q_1$ et R conviennent.

Le résultat est démontré par récurrence.

Unicité. Soit $(Q_1, Q_2, R_1, R_2) \in \mathbb{K}[X]^4$ et $A = BQ_1 + R_1 = BQ_2 + R_2$ et $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$.
On a donc $B(Q_1 - Q_2) = R_2 - R_1$ avec $\deg(R_2 - R_1) \leqslant \operatorname{Max}\{\deg(R_1), \deg(R_2)\} < \deg(B)$.
Si $Q_1 \neq Q_2$, alors $Q_1 - Q_2$ a un degré entier puis

$$\deg(R_2 - R_1) = \deg(B(Q_1 - Q_2)) = \deg(B) + \deg(Q_1 - Q_2) \geqslant \deg(B)$$

ce qui est faux. Donc, $Q_1 = Q_2$ puis $R_1 = R_2$.

❑

Définition 7. Les polynômes Q et R du théorème 18 sont respectivement le **quotient** de la division euclidienne de A par B et le **reste** de la division euclidienne de A par B.

Dans la démonstration par récurrence effectuée plus haut, on a au passage dégagé la méthode pour effectuer une division euclidienne « petit à petit ». Explicitons sur un exemple la technique mise en œuvre.

- Soient $A = 3X^5 - X^4 + 3X^2 + X + 1$ et $B = 2X^3 - 5X^2 + X + 4$.

On doit commencer par considérer $A - \dfrac{3}{2}X^2 B$ ($A - \dfrac{a_{n+1}}{b_m} X^{n+1-m} B$ dans le cas général) :

$$\begin{aligned} A - \frac{3}{2}X^2 B &= 3X^5 - X^4 + 3X^2 + X + 1 - \frac{3}{2}X^2 \left(2X^3 - 5X^2 + X + 4 \right) \\ &= \frac{13}{2}X^4 - \frac{3}{2}X^3 - 3X^2 + X + 1. \end{aligned}$$

Le polynôme $A-\frac{3}{2}X^2B$ est de degré au plus $\deg(A)-1=4$ et on recommence tant que l'on n'a pas a obtenu un polynôme de degré au plus $\deg(B)-1=2$.

$$\begin{aligned}A-\left(\frac{3}{2}X^2+\frac{13}{4}X\right)B&=\frac{13}{2}X^4-\frac{3}{2}X^3-3X^2+X+1-\frac{13}{4}X\left(2X^3-5X^2+X+4\right)\\&=\frac{59}{4}X^3-\frac{25}{4}X^2-12X+1.\end{aligned}$$

puis

$$\begin{aligned}A-\left(\frac{3}{2}X^2+\frac{13}{4}X+\frac{59}{8}\right)B&=\frac{59}{4}X^3-\frac{25}{4}X^2-12X+1-\frac{59}{8}\left(2X^3-5X^2+X+4\right)\\&=\frac{245}{8}X^2-\frac{155}{8}X-\frac{57}{2}.\end{aligned}$$

Ceci s'écrit encore $A=\left(\frac{3}{2}X^2+\frac{13}{4}X+\frac{59}{8}\right)B+\frac{245}{8}X^2-\frac{155}{8}X-\frac{57}{2}$. Le quotient de la division euclidienne de A par B est $Q=\frac{3}{2}X^2+\frac{13}{4}X+\frac{59}{8}$ et le reste de la division euclidienne de A par B est $R=\frac{245}{8}X^2-\frac{155}{8}X-\frac{57}{2}$.

• Tout ce qui précède est lourd à manipuler. On va mettre en place une technique bien plus légère. Effectuons la division euclidienne de $A=X^4-4X^3+X+2$ par $B=X^2-3X+5$. On dispose les différents objets de la façon suivante (on obtiendra le quotient en bas à droite et le reste en bas à gauche) :

$A=$ dividende	$B=$ diviseur
$R=$ reste	$Q=$ quotient

En analysant les termes de plus haut degré des polynômes A et B : « il y va X^2 fois ». On écrit X^2 dans la zone en bas à droite, on calcule X^2B et on écrit le résultat de ce produit dans la zone en bas à gauche en prenant soin d'aligner verticalement les monômes de même degré (on a donc laissé un espace vide dans le polynôme A pour tenir compte de l'absence de X^2) et on soustrait

$X^4-4X^3+\quad+X+2$	X^2-3X+5
$-\left(X^4-3X^3+5X^2\right)$	X^2
$-X^3-5X^2+X+2$	

puis on recommence

$X^4-4X^3+\quad+X+2$	X^2-3X+5
$-\left(X^4-3X^3+5X^2\right)$	X^2-X
$-X^3-5X^2+X+2$	
$-\left(-X^3+3X^2-5X\right)$	
$-8X^2+6X+2$	

et finalement (la division s'arrête quand le reste a un degré strictement inférieur au degré du diviseur)

$$\begin{array}{l|l}
X^4-4X^3+\quad +X+2 & X^2-3X+5 \\
\hline
-\left(X^4-3X^3+5X^2\right) & X^2-X-8 \\
\cline{1-1}
\quad -X^3-5X^2+X+2 & \\
-\left(-X^3+3X^2-5X\right) & \\
\cline{1-1}
\quad\quad -8X^2+6X+2 & \\
\quad -\left(-8X^2+24X-40\right) & \\
\cline{1-1}
\quad\quad -18X+42 &
\end{array}$$

Le bilan de cette division est : $X^4-4X^3+X+2=\left(X^2-X-8\right)\left(X^2-3X+5\right)-18X+42$. Le quotient est $Q=X^2-X-8$ et le reste est $R=-18X+42$. Une fois que le mécanisme est compris, cette disposition de la division peut encore être allégée en

$$\begin{array}{l|l}
X^4-4X^3+\quad +X+2 & X^2-3X+5 \\
\hline
\quad -X^3-5X^2+X+2 & X^2-X-8 \\
\quad\quad -8X^2+6X+2 & \\
\quad\quad -18X+42 &
\end{array}$$

Exercice 4. Pour $n\in\mathbb{N}^*$, on pose $P_n=X^n-1$. Effectuer la division euclidienne de P_n par P_m.

Solution 4. Soit $(m,n)\in\left(\mathbb{N}^*\right)^2$. La division euclidienne de n par m s'écrit $n=qm+r$ où $(q,r)\in\mathbb{N}^2$ et $0\leqslant r<m$.

$$\begin{aligned}
X^n-1=X^{qm+r}-1&=X^{qm+r}-X^r+X^r-1=X^r\left((X^m)^q-1\right)+X^r-1\\
&=X^r\left(1+X^m+(X^m)^2+\ldots+(X^m)^{q-1}\right)(X^m-1)+X^r-1.
\end{aligned}$$

Puisque $\deg\left(X^r-1\right)\leqslant r<m$ (si $r\geqslant 1$, $\deg\left(X^r-1\right)=r$ et si $r=0$, $\deg\left(X^r-1\right)=-\infty$), la division euclidienne est achevée. Le quotient est $Q=X^r\left(1+X^m+(X^m)^2+\ldots+(X^m)^{q-1}\right)$ et le reste est $R=X^r-1$.

2.2 Divisibilité dans $\mathbb{K}[X]$

2.2.1 Définition de la divisibilité

Définition 8. Soient A et B deux éléments de $\mathbb{K}[X]$, B étant non nul.

B **divise** A si et seulement si il existe $Q\in\mathbb{K}[X]$ tel que $A=BQ$. On écrit dans ce cas $B|A$.

Soient A et B deux éléments de $\mathbb{K}[X]$.

A **est multiple de** B si et seulement si il existe $Q\in\mathbb{K}[X]$ tel que $A=BQ$.

Notation. L'ensemble des multiples d'un polynôme A se note $A\times\mathbb{K}[X]$ ou plus simplement $A\mathbb{K}[X]$:

$$A\mathbb{K}[X]=\{AQ,\ Q\in\mathbb{K}[X]\}.$$

Exemple. Le polynôme $X-1$ divise le polynôme $X^2-3X+2=(X-1)(X-2)$ avec $X-2\in\mathbb{K}[X]$. Le polynôme $X-1$ divise le polynôme $2X-2$ car $2X-2=2(X-1)$ avec $2\in\mathbb{K}[X]$ et $2X-2$ divise $X-1$ car $X-1=\frac{1}{2}(2X-2)$ avec $\frac{1}{2}\in\mathbb{K}[X]$. Les polynômes $A=X-1$ et $B=2X-2$ sont un exemple de polynômes A et B tels que $A|B$ et $B|A$.

2.2.2 Propriétés de la divisibilité

Un résultat immédiat est :

Théorème 19. Soient A un polynôme et B un polynôme non nul.

B divise A si et seulement si le reste de la division euclidienne de A par B est nul.

Théorème 20.

- $\forall A \in \mathbb{K}[X] \setminus \{0\}$, $A|A$.
- $\forall (A, B, C) \in (\mathbb{K}[X] \setminus \{0\}) \times (\mathbb{K}[X] \setminus \{0\}) \times \mathbb{K}[X]$, $(A|B \text{ et } B|C) \Rightarrow A|C$.

Démonstration .

- Soit $A \in \mathbb{K}[X] \setminus \{0\}$. $A = 1 \times A$ avec $1 \in \mathbb{K}[X]$. Donc, $A|A$.
- Soit $(A, B, C) \in (\mathbb{K}[X] \setminus \{0\}) \times (\mathbb{K}[X] \setminus \{0\}) \times \mathbb{K}[X]$ tel que $A|B$ et $B|C$. Il existe $(Q_1, Q_2) \in \mathbb{K}[X]^2$ tel que $B = Q_1 A$ et $C = Q_2 B$. Mais alors, $C = Q_2 Q_1 A$ avec $Q_2 Q_1 \in \mathbb{K}[X]$ et donc $A|C$.

❑

Ainsi, la relation de divisibilité est réflexive et transitive. Par contre, la relation de divisibilité n'est pas anti-symétrique. C'est ce qu'analyse le théorème suivant :

Théorème 21. $\forall (A, B) \in (\mathbb{K}[X] \setminus \{0\})^2$, $(A|B \text{ et } B|A) \Leftrightarrow \exists \lambda \in \mathbb{K} \setminus \{0\} / \ B = \lambda A$.

Démonstration . Soit $(A, B) \in (\mathbb{K}[X] \setminus \{0\})^2$.

$\Leftarrow /$. Supposons qu'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $B = \lambda A$. Soient $Q_1 = \lambda \in \mathbb{K}[X]$ et $Q_2 = \dfrac{1}{\lambda} \in \mathbb{K}[X]$. On a $B = Q_1 A$ et $A = Q_2 B$ et donc $A|B$ et $B|A$.

$\Rightarrow /$. Supposons que $A|B$ et $B|A$. Il existe $(Q_1, Q_2) \in \mathbb{K}[X]^2$ tel que $B = Q_1 A$ et $A = Q_2 B$. Mais alors, $A = Q_2 Q_1 A$ puis $Q_1 Q_2 = 1$ car $A \neq 0$. Les polynômes Q_1 et Q_2 sont des inversibles de l'anneau $(\mathbb{K}[X], +, \times)$ et donc, d'après le théorème 8, Q_1 et Q_2 sont des constantes non nulles. Ainsi, il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $B = \lambda A$.

❑

Théorème 22. Soient A et B deux polynômes non nuls tels que $B|A$. Alors, $\deg(B) \leqslant \deg(A)$.

Démonstration . Il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. Puisque $A \neq 0$, on a nécessairement $Q \neq 0$ puis $\deg(A)$, $\deg(B)$ et $\deg(Q)$ sont des entiers naturels. Mais alors,

$$\deg(A) = \deg(QB) = \deg(Q) + \deg(B) \geqslant \deg(B).$$

❑

Théorème 23. Soient A, B et C trois polynômes tels que $A \neq 0$, $A|B$ et $A|C$. Alors, pour tout $(P_1, P_2) \in \mathbb{K}[X]^2$, $A|(P_1 B + P_2 C)$.

Démonstration . Il existe $(Q_1, Q_2) \in \mathbb{K}[X]^2$ tel que $B = AQ_1$ et $C = AQ_2$ Mais alors, $P_1 B + P_2 C = (P_1 Q_1 + P_2 Q_2) A$ avec $P_1 Q_1 + P_2 Q_2 \in \mathbb{K}[X]$. Donc, $A|(P_1 B + P_2 C)$.

❑

2.3 PGCD

2.3.1 Définition du PGCD de deux polynômes non nuls

Les quelques théorèmes qui suivent préparent la définition du PGCD de deux polynômes non nuls.

Si P est un polynôme, on note $\text{div}(P)$ l'ensemble des diviseurs de P (un élément de $\text{div}(P)$ est par définition non nul).

Théorème 24. Soit P un polynôme. Alors, pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, $\text{div}(\lambda P) = \text{div}(P)$.

Démonstration. Soit P un polynôme. Soit D un polynôme non nul élément de $\text{div}(P)$. Il existe un polynôme Q tel que $P = QD$. Mais alors, $\lambda P = (\lambda Q)D$ et donc D est élément de $\text{div}(\lambda P)$.
Ainsi, pour tout polynôme P et tout λ de $\mathbb{K} \setminus \{0\}$, $\text{div}(P) \subset \text{div}(\lambda P)$. Mais alors, pour $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K} \setminus \{0\}$, on a aussi $\text{div}(\lambda P) \subset \text{div}\left(\frac{1}{\lambda}\lambda P\right) = \text{div}(P)$.

Finalement, pour tout $P \in \mathbb{K}[X]$ et tout $\lambda \in \mathbb{K} \setminus \{0\}$, $\text{div}(\lambda P) = \text{div}(P)$.

❑

Théorème 25. Soit P un polynôme. Pour tout polynôme D non nul, si $D \in \text{div}(P)$, alors pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, $\lambda D \in \text{div}(P)$.

Démonstration. Soit P un polynôme. Soient D un polynôme non nul élément de $\text{div}(P)$ et $\lambda \in \mathbb{K} \setminus \{0\}$. Il existe un polynôme Q tel que $P = QD$. Mais alors, $\lambda P = Q(\lambda D)$ et donc λD est élément de $\text{div}(\lambda P) = \text{div}(P)$. ❑

Théorème 26. Soient A et B deux polynômes non nuls. Il existe un polynôme unitaire D_0 de degré maximum qui divise à la fois A et B.

⇨ **Commentaire.** *Dire que D_0 est un diviseur commun à A et à B, de degré maximum, signifie que D_0 est un diviseur commun à A et à B et que tout diviseur commun à A et à B a un degré inférieur ou égal au degré de D_0.*

Démonstration. Soit $\mathcal{E} = \{D \in \mathbb{K}[X] \setminus \{0\} / \ D|A \text{ et } D|B\}$ puis $\mathcal{D} = \{\deg(D),\ D \in \mathcal{E}\}$.
Tout élément de $\mathcal{E}$ a un degré qui est un entier naturel inférieur ou égal à $\deg(A)$ et $\deg(B)$ et donc à $\text{Min}\{\deg(A), \deg(B)\}$. D'autre part, $\mathcal{E}$ n'est pas vide car $1 \in \mathcal{E}$. $\mathcal{D}$ est donc une partie non vide et majorée de $\mathbb{N}$ et à ce titre admet un plus grand élément d. Soit D un élément de $\mathcal{E}$ de degré d. D est un polynôme qui est un diviseur commun à A et B de degré maximum .

Soit $D_0 = \frac{1}{\text{dom}(D)}D$. D'après le théorème 25, D_0 est un diviseur commun à A et B. Enfin, D_0 est de même degré que D et donc le degré de D_0 est le maximum des degrés des diviseurs communs à A et à B

❑

Les deux théorèmes qui suivent ont entre autre pour but d'établir l'unicité de D_0.

Théorème 27 (lemme d'Euclide). Soient A, B, Q et R quatre polynômes tels que $A = BQ + R$.

Alors, $\text{div}(A) \cap \text{div}(B) = \text{div}(B) \cap \text{div}(R)$.

Démonstration. Soit $D \in \text{div}(A) \cap \text{div}(B)$. Alors, D divise B et $R = A - BQ$ d'après le théorème 23 et donc $D \in \text{div}(B) \cap \text{div}(R)$.
Inversement, soit $D \in \text{div}(B) \cap \text{div}(R)$. Alors, D divise B et $A = BQ + R$ et donc $D \in \text{div}(A) \cap \text{div}(B)$.

On a montré que $\text{div}(A) \cap \text{div}(B) = \text{div}(B) \cap \text{div}(R)$. ❑

Théorème 28. Soient A et B deux polynômes non nuls. Soit D_0 un polynôme unitaire, diviseur commun à A et B, de degré maximum.

Alors, $\text{div}(A) \cap \text{div}(B) = \text{div}(D_0)$.

Démonstration. Puisque D_0 divise A et B, un diviseur D de D_0 divise A et B par transitivité ou encore un diviseur de D_0 est un diviseur commun à A et B. Ceci montre que $\text{div}(D_0) \subset \text{div}(A) \cap \text{div}(B)$.

Inversement, montrons que $\text{div}(A) \cap \text{div}(B) \subset \text{div}(D_0)$. Plus précisément, montrons par récurrence forte que pour tout $n \in \mathbb{N}$, pour tous polynômes non nuls A et B tels que $\deg(B) = n$, un diviseur commun à A et B est un diviseur de D_0 où D_0 est un polynôme unitaire, diviseur commun à A et B de degré maximum.

- Si $n = 0$, un diviseur commun à A et à B est en particulier un diviseur de B et est donc un polynôme de degré 0.
Un tel polynôme divise D_0.

- Soit $n \geqslant 0$. Supposons que pour tout $k \in [\![0, n]\!]$, pour tous polynômes non nuls A et B tels que $\deg(B) = k$, un diviseur commun à A et B est un diviseur de D_0 où D_0 est un polynôme unitaire, diviseur commun à A et B de degré maximum.
Soient A et B deux polynômes non nuls tels que $\deg(B) = n + 1$. Soit D_0 un polynôme unitaire de degré maximum, diviseur commun à A et B.
La division euclidienne de A par B s'écrit $A = BQ + R$ où Q et R sont deux polynômes tels que $\deg(R) \leqslant \deg(B) - 1 = n$. D'après le lemme d'Euclide, D_0 est aussi un polynôme unitaire de degré maximum, diviseur commun à B et R.
Par hypothèse de récurrence, puisque $\deg(R) \leqslant n$, un diviseur commun à A et B, qui est aussi un diviseur commun à B et R, est

un diviseur de D_0. Donc, $\text{div}(A) \cap \text{div}(B) \subset \text{div}(D_0)$.

Le résultat est démontré par récurrence.

❑

On résume et on complète les théorèmes précédents qui établissent l'existence et l'unicité du PGCD unitaire de deux polynômes non nuls.

Théorème 29. Soient A et B deux polynômes non nuls.

1) Il existe un polynôme unitaire D_0 et un seul, diviseur commun à A et à B, de degré maximum.

2) $\text{div}(A) \cap \text{div}(B) = \text{div}(D_0)$.

3) Pour tout polynôme non nul D, D est un polynôme de degré maximum, diviseur commun à A et à B si et seulement si il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $D = \lambda D_0$ si et seulement si $\text{div}(A) \cap \text{div}(B) = \text{div}(D)$.

Démonstration .

1) Le théorème 26 établit l'existence de D_0. Soit alors D_1 un polynôme unitaire, diviseur commun à A et à B, de degré maximum. D'après le théorème 28, $\text{div}(D_1) = \text{div}(A) \cap \text{div}(B) = \text{div}(D_0)$.
En particulier, $D_1 \in \text{div}(D_1) = \text{div}(D_0)$ et $D_0 \in \text{div}(D_0) = \text{div}(D_1)$. Ainsi, $D_1 | D_0$ et $D_0 | D_1$. Donc, d'après le théorème 21, il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $D_1 = \lambda D_0$. Enfin, D_0 et D_1 sont unitaires et donc

$$1 = \text{dom}(D_1) = \text{dom}(\lambda D_0) = \lambda \text{dom}(D_0) = \lambda$$

puis $D_1 = D_0$. Ceci montre l'unicité de D_0.

2) C'est le théorème 28 que l'on a rappelé.

3) • Soit D un polynôme non nul tel que $\text{div}(D) = \text{div}(A) \cap \text{div}(B) = \text{div}(D_0)$, comme en 1), D divise D_0 et D_0 divise D. Par suite, il existe $\lambda \neq 0$ tel que $D = \lambda D_0$.
Réciproquement, supposons que $D = \lambda D_0$, $\lambda \neq 0$. D'après le théorème 24, $\text{div}(D) = \text{div}(D_0)$.
On a montré que $\text{div}(D) = \text{div}(A) \cap \text{div}(B)$ si et seulement si il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $D = \lambda D_0$.

• Supposons $\text{div}(A) \cap \text{div}(B) = \text{div}(D)$. $D \in \text{div}(D) = \text{div}(A) \cap \text{div}(B)$ est un diviseur commun à A et B. De plus, D est un polynôme de degré maximum de $\text{div}(D) = \text{div}(A) \cap \text{div}(B)$.
Finalement, D est un polynôme de degré maximum, diviseur commun à A et B.

Réciproquement, soit D un polynôme non nul, diviseur commun à A et à B, de degré maximum. D est donc un élément de $\text{div}(A) \cap \text{div}(B) = \text{div}(D_0)$ de degré maximum et en particulier, D est un diviseur de D_0, de même degré que D_0. On en déduit qu'il existe $\lambda \neq 0$ tel que $D = \lambda D_0$ puis que $\text{div}(A) \cap \text{div}(B) = \text{div}(D_0) = \text{div}(D)$.

❑

On peut maintenant énoncer :

Définition 9. Soient A et B deux polynômes non nuls.

Le polynôme unitaire, diviseur commun à A et à B de degré maximum, s'appelle **le PGCD unitaire** de A et B (ou plus simplement le PGCD de A et B). Il se note $A \wedge B$.

Tout polynôme de la forme $\lambda(A \wedge B)$, $\lambda \in \mathbb{K} \setminus \{0\}$, s'appelle **un PGCD** de A et B.

Par exemple, même si nous n'avons pas encore à disposition des outils efficaces pour déterminer le PGCD de deux polynômes, il est clair que $[(X-1)(X-2)(X-3)] \wedge [(X-1)(X-2)(X-4)] = (X-1)(X-2)$ ou que si $a \neq b$, $(X-a) \wedge (X-b) = 1$.

⇨ **Commentaire .**

◇ *On note que le théorème 29 fournit plus explicitement : div*$(A) \cap$ *div*$(B) =$ *div*$(A \wedge B)$ *ou encore*

les diviseurs communs à deux polynômes non nuls sont les diviseurs de leur PGCD.

◇ *Le théorème 27 dit en particulier que si* A *et* B *sont deux polynômes non nuls et* Q *et* R *sont deux polynômes tels que* $A = BQ + R$ *et* $R \neq 0$*, alors*

$$A \wedge B = B \wedge R.$$

◇ *Les PGCD de* A *et* B *sont les polynômes de la forme* $\lambda(A \wedge B)$*,* $\lambda \in \mathbb{K} \setminus \{0\}$.

◇ *Si* λ *et* μ *sont non nuls, div*$(\lambda A) \cap$ *div*$(\mu B) =$ *div*$(A) \cap$ *div*$(B) =$ *div*$(A \cap B)$ *et en particulier,* $(\lambda A) \wedge (\mu B) = A \wedge B$.

2.3.2 Algorithme d'Euclide

• On se donne A et B deux polynômes non nuls tels que $\deg(A) \geqslant \deg(B)$. On commence par effectuer la division euclidienne de $R_0 = A$ par $R_1 = B$: $R_0 = Q_0R_1 + R_2$ avec $(Q_0, R_2) \in \mathbb{K}[X]^2$ et $\deg(R_2) < \deg(R_1) = \deg(B)$ et plus généralement, pour $k \in \mathbb{N}$, tant que $R_{k+1} \neq 0$, on effectue la division euclidienne de R_k par R_{k+1} :

$$R_k = Q_kR_{k+1} + R_{k+2}$$

avec $(Q_k, R_{k+2}) \in \mathbb{K}[X]^2$ et $\deg(R_{k+2}) < \deg(R_{k+1})$.

• Si, par l'absurde, l'algorithme précédent ne s'arrête pas, la suite $(\deg(R_k))_{k\in\mathbb{N}^*}$ est une suite strictement décroissante d'entiers naturels. Une telle suite n'existe pas, comme on l'a déjà vu dans le chapitre « Arithmétique dans $\mathbb{Z}$ ». Donc, l'algorithme d'Euclide s'arrête ou encore, il existe un premier reste nul. On note $k_0 + 2$ son numéro.

• D'après le lemme d'Euclide,

$$A \wedge B = R_0 \wedge R_1 = \ldots = R_{k_0} \wedge R_{k_0+1}.$$

Enfin, puisque par définition $R_{k_0+2} = 0$, on a $R_{k_0} = Q_{k_0}R_{k_0+1}$ où Q_{k_0} est un certain polynôme non nul. R_{k_0+1} est alors un diviseur commun à R_{k_0} et R_{k_0+1}, de degré maximum et donc R_{k_0+1} est un PGCD de R_{k_0} et R_{k_0+1} ou aussi $\dfrac{1}{\mathrm{dom}(R_{k_0+1})}R_{k_0+1}$ est le PGCD unitaire de R_{k_0} et R_{k_0+1} et donc de A et B.

Notons que si, au début de l'algorithme, on a $\deg(B) > \deg(A)$, la première division de A par B a un quotient nul et un reste égal à A puis la deuxième division est la division de B par A où cette fois-ci $\deg(B) > \deg(A)$

On peut énoncer :

Théorème 30. Soient A et B deux polynômes non nuls. On pose $R_0 = A$ et $R_1 = B$ puis, tant que $R_{k+1} \neq 0$, $R_k = Q_kR_{k+1} + R_{k+2}$ avec $(Q_k, R_{k+2}) \in \mathbb{K}[X]^2$ et $\deg(R_{k+2}) < \deg(R_{k+1})$.

• Il existe un premier reste nul ou encore l'algorithme s'arrête.

• Un PGCD de A et B est le dernier reste non nul.

Exercice 4. Trouver le PGCD de $A = X^4 + X^3 + 2X^2 + X + 1$ et $B = X^3 - 3X^2 + X - 3$.

Solution 4. $X^4 + X^3 + 2X^2 + X + 1 = (X + 4)\left(X^3 - 3X^2 + X - 3\right) + 13X^2 + 13$.
Donc, $A \wedge B = \left(X^3 - 3X^2 + X - 3\right) \wedge \left(13X^2 + 13\right) = \left(X^3 - 3X^2 + X - 3\right) \wedge \left(X^2 + 1\right)$.

$X^3 - 3X^2 + X - 3 = (X - 3)\left(X^2 + 1\right)$. Ainsi, le polynôme $X^2 + 1$ divise le polynôme $X^3 - 3X^2 + X - 3$. Donc, l'algorithme s'arrête et $A \wedge B = \left(X^3 - 3X^2 + X - 3\right) \wedge \left(X^2 + 1\right) = X^2 + 1$.

Comme dans le chapitre « Arithmétique dans $\mathbb{Z}$ » (théorème 16), la détermination de $A \wedge B$ par l'algorithme d'Euclide fournit :

Théorème 31. Soient A et B deux polynômes non nuls.

Il existe $(U, V) \in \mathbb{K}[X]$ tel que $A \wedge B = AU + BV$.

Démonstration. Si B divise A, un PGCD de A et B est B ou encore $A \wedge B = \dfrac{1}{\mathrm{dom}(B)}B = 0 \times A + \dfrac{1}{\mathrm{dom}(B)}B$. Dans ce cas, les polynômes $U = 0$ et $V = \dfrac{1}{\mathrm{dom}(B)}$ conviennent.

Sinon, avec les notations de l'algorithme d'Euclide exposé plus haut, on a $A \wedge B = \dfrac{1}{\mathrm{dom}(R_{k_0+1})}R_{k_0+1}$. A partir de l'égalité, $R_{k_0-1} = Q_{k_0-1}R_{k_0} + R_{k_0+1}$, on obtient une égalité de la forme

$$A \wedge B = \frac{1}{\mathrm{dom}(R_{k_0+1})}R_{k_0+1} = R_{k_0-1}U_{k_0-1} + R_{k_0}V_{k_0-1}$$

où $U_{k_0-1} = \dfrac{1}{\mathrm{dom}(R_{k_0+1})}$ et $V_{k_0-1} = -\dfrac{1}{\mathrm{dom}(R_{k_0+1})}Q_{k_0-1}$ sont des polynômes. Puis en remontant dans l'algorithme, par récurrence, on peut écrire $A \wedge B$ sous la forme

$$A \wedge B = R_kU_k + R_{k+1}V_k$$

pour tout $k \in [\![0, k_0 - 1]\!]$, où U_k et V_k sont des polynômes. En particulier, pour $k = 0$, il existe deux polynômes U et V tels que

$$A \wedge B = R_0 U + R_1 V = AU + BV.$$

❑

Exercice 5. Déterminer deux polynômes U et V tels que $U \times \left(X^2+X+1\right) + V \times \left(X^2-X+1\right) = 1$.

Solution 5. $X^2+X+1 = 1 \times \left(X^2-X+1\right) + 2X$ puis $X^2-X+1 = \left(\frac{X}{2} - \frac{1}{2}\right)(2X) + 1$. Donc,

$$\begin{aligned} 1 &= \left(X^2-X+1\right) - \left(\frac{X}{2} - \frac{1}{2}\right)(2X) \\ &= \left(X^2-X+1\right) - \left(\frac{X}{2} - \frac{1}{2}\right)\left[\left(X^2+X+1\right) - \left(X^2-X+1\right)\right] \\ &= \left(-\frac{X}{2} + \frac{1}{2}\right)\left(X^2+X+1\right) + \left(\frac{X}{2} + \frac{1}{2}\right)\left(X^2-X+1\right). \end{aligned}$$

Les polynômes $U = -\frac{X}{2} + \frac{1}{2}$ et $V = \frac{X}{2} + \frac{1}{2}$.

2.3.3 Propriétés du PGCD de deux polynômes

Un résultat immédiat est :

Théorème 32. Pour tout $A \in \mathbb{K}[X] \setminus \{0\}$, $A \wedge A = \frac{1}{\mathrm{dom}(A)} A$.

D'autre part, on a déjà eu l'occasion de vérifier que :

Théorème 33. Pour tout $(A,B) \in (\mathbb{K}[X] \setminus \{0\})^2$ et tout $(\lambda,\mu) \in (\mathbb{K} \setminus \{0\})^2$, $(\lambda A) \wedge (\mu B) = A \wedge B$.

Théorème 34.

1) $\forall (A,B) \in (\mathbb{K}[X] \setminus \{0\})^2$, $A \wedge B = B \wedge A$ (commutativité du PGCD).

2) $\forall (A,B,C) \in (\mathbb{K}[X] \setminus \{0\})^3$, $(A \wedge B) \wedge C = A \wedge (B \wedge C)$ (associativité du PGCD).

3) $\forall A \in \mathbb{K}[X] \setminus \{0\}$, $A \wedge 1 = 1$ (1 est absorbant).

Démonstration .

1) Soit $(A,B) \in (\mathbb{K}[X] \setminus \{0\})^2$. On a $\mathrm{div}(A) \cap \mathrm{div}(B) = \mathrm{div}(B) \cap \mathrm{div}(A)$. En particulier, $A \wedge B = B \wedge A$.

2) Soit $(A,B,C) \in (\mathbb{K}[X] \setminus \{0\})^3$.

$$\mathrm{div}((A \wedge B) \wedge C) = \mathrm{div}(A \wedge B) \cap \mathrm{div}(C) = \mathrm{div}(A) \cap \mathrm{div}(B) \cap \mathrm{div}(C) = \mathrm{div}(A) \cap \mathrm{div}(B \wedge C) = \mathrm{div}(A \wedge (B \wedge C))$$

et en particulier, $(A \wedge B) \wedge C = A \wedge (B \wedge C)$. On peut donc dorénavant écrire $A \wedge B \wedge C$.

3) $A \wedge 1$ est en particulier un diviseur unitaire de 1. Donc, $A \wedge 1 = 1$.

❑

Théorème 35. $\forall (A,B,C) \in (\mathbb{K}[X] \setminus \{0\})^3$, C étant unitaire. Alors, $(CA) \wedge (CB) = C(A \wedge B)$.

Démonstration . C divise CA et CB et donc C divise $(CA) \wedge (CB)$. Il existe un polynôme non nul Q tel que $(CA) \wedge (CB) = CQ$.

CQ divise CA et donc Q divise A ($CA = Q_1 CQ$ puis $A = Q_1 Q$ car $C \neq 0$). De même, Q divise B et donc Q divise $A \wedge B$.
Inversement, $C(A \wedge B)$ divise CA et CB puis $C(A \wedge B)$ divise $(CA) \wedge (CB) = CQ$ et finalement $A \wedge B$ divise Q.

En résumé, Q divise $A \wedge B$ et $A \wedge B$ divise Q. Donc, il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $Q = \lambda(A \wedge B)$. Enfin, CQ est unitaire car égal à $(CA) \wedge (CB)$ et C est unitaire. Donc Q est unitaire puis $\lambda = 1$ puis $Q = A \wedge B$ et finalement $(CA) \wedge (CB) = C(A \wedge B)$.

❑

Théorème 36. $\forall (A,B) \in (\mathbb{K}[X]\setminus\{0\})^3$. En posant $D = A \wedge B$, il existe $(A_1, A_2) \in (\mathbb{K}[X]\setminus\{0\})^2$ tel que $A = DA_1$ et $B = DB_1$ et $A_1 \wedge B_1 = 1$.

Démonstration. Puisque D divise A et B, il existe deux polynômes A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. De plus, $D = A \wedge B = (DA_1) \wedge (DB_1) = D(A_1 \wedge B_1)$ puis $A_1 \wedge B_1 = 1$ après simplification par le polynôme non nul D.

❑

2.3.4 PGCD de plusieurs polynômes

De nouveau, on prépare la définition du PGCD de plusieurs polynômes. On peut démontrer par récurrence (et nous ne le ferons pas) que :

Théorème 37. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

1) Il existe un et un seul polynôme unitaire D_0 qui divise $A_1, \ldots, A_n$ et de degré maximum.
De plus, $\text{div}(A_1) \cap \ldots \cap \text{div}(A_n) = \text{div}(D_0)$.

2) Les polynômes D, diviseurs communs à $A_1, \ldots, A_n$, et de degré maximum, sont les polynômes de la forme λD_0, $\lambda \in \mathbb{K}\setminus\{0\}$.

On peut alors poser :

Définition 10. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

Le polynôme unitaire, diviseur commun à $A_1, \ldots, A_n$ de degré maximum, s'appelle **le PGCD unitaire** de $A_1, \ldots, A_n$ (ou plus simplement le PGCD de $A_1, \ldots, A_n$). Il se note $A_1 \wedge \ldots \wedge A_n$.

Tout polynôme de la forme $\lambda(A_1 \wedge \ldots \wedge A_n)$, $\lambda \in \mathbb{K}\setminus\{0\}$, s'appelle **un PGCD** de $A_1, \ldots, A_n$.

Le théorème 37 dit que $\text{div}(A_1) \cap \ldots \cap \text{div}(A_n) = \text{div}(A_1 \wedge \ldots \wedge A_n)$ ou encore

les diviseurs communs à n polynômes non nuls sont les diviseurs de leur PGCD.

Ensuite, on peut montrer par récurrence (et nous ne le ferons pas) que :

Théorème 38. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

Il existe n polynômes $U_1, \ldots, U_n$, tels que $A_1U_1 + \ldots + A_nU_n = A_1 \wedge \ldots \wedge A_n$.

Notons enfin que l'associativité du PGCD fournit par récurrence : $A_1 \wedge \ldots \wedge A_{n-1} \wedge A_n = (A_1 \wedge \ldots \wedge A_{n-1}) \wedge A_n$.

2.4 PPCM

2.4.1 Définition du PPCM de deux polynômes

On s'intéresse maintenant aux multiples communs à deux polynômes A et B. On rappelle que l'ensemble des multiples d'un polynôme A se note $A\,\mathbb{K}[X] : A\,\mathbb{K}[X] = \{AQ,\ Q \in \mathbb{K}[X]\}$. On s'intéresse donc à l'ensemble $(A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X])$.

Théorème 39. Soient A et B deux polynômes non nuls. Il existe un polynôme unitaire M_0 et un seul tel que $(A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X]) = M_0\,\mathbb{K}[X]$.

Démonstration.

Existence.

• Soit $\mathcal{D} = \{\deg(M),\ M \in ((A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X]))\setminus\{0\}\}$. Le polynôme AB est un multiple commun à A et B qui n'est pas nul. Donc, $\mathcal{D}$ est une partie non vide de $\mathbb{N}$ et à ce titre, $\mathcal{D}$ admet un plus petit élément m. Soit M un élément de $((A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X]))\setminus\{0\}$ de degré m puis $M_0 = \dfrac{1}{\text{dom}(M)}M$. M_0 est un polynôme unitaire, multiple commun à A et B.

• Soit $M \in M_0\,\mathbb{K}[X]$. M est un multiple de M_0 et M_0 est un multiple de A. Donc, M est un multiple de A. De même, M est un multiple de B et finalement $M \in (A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X])$. Ceci montre que $M_0\,\mathbb{K}[X] \subset (A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X])$.

• Inversement, soit $M \in (A\,\mathbb{K}[X]) \cap (B\,\mathbb{K}[X])$. La division euclidienne de M par M_0 s'écrit $M = QM_0 + R$ avec $(Q,R) \in \mathbb{K}[X]^2$ et $\deg(R) < \deg(M_0)$.
M est un multiple de A et QM_0 est un multiple de A. Donc, $R = M - QM_0$ est un multiple de A ($R = M - QM_0 = Q_1A - Q_2A = (Q_1 - Q_2)A$). De même, R est un multiple de B. Donc, R est un multiple commun à A et B de degré strictement inférieur au degré de M_0. Par définition de M_0, il ne reste que $R = 0$ et donc $M = QM_0 \in M_0\,\mathbb{K}[X]$.

Ainsi, $(A\,\mathbb{K}[X])\cap(B\,\mathbb{K}[X])\subset M_0\,\mathbb{K}[X]$ et finalement, $(A\,\mathbb{K}[X])\cap(B\,\mathbb{K}[X])=M_0\,\mathbb{K}[X]$. On a montré l'existence de M_0.

Unicité. Soit M_1 un polynôme unitaire tel que $M_1\,\mathbb{K}[X]=(A\,\mathbb{K}[X])\cap(B\,\mathbb{K}[X])=M_0\,\mathbb{K}[X]$. Alors, $M_1\in M_1\,\mathbb{K}[X]=M_0\,\mathbb{K}[X]$ et $M_0\in M_0\,\mathbb{K}[X]=M_1\,\mathbb{K}[X]$. Donc, M_0 est un multiple de M_1 et M_1 est un multiple de M_0. On sait alors qu'il existe $\lambda\in\mathbb{K}\setminus\{0\}$ tel que $M_1=\lambda M_0$. De plus, M_0 et M_1 sont unitaires et donc

$$1=\text{dom}\,(M_1)=\text{dom}\,(\lambda M_0)=\lambda\text{dom}\,(M_0)=\lambda$$

puis $M_1=M_0$. Ceci montre l'unicité de M_0.

❑

Théorème 40. Soient A et B deux polynômes non nuls.

Pour tout polynôme M, $(A\,\mathbb{K}[X])\cap(B\,\mathbb{K}[X])=M\,\mathbb{K}[X]\Leftrightarrow\exists\lambda\in\mathbb{K}\setminus\{0\}/\ M=\lambda M_0$.

Démonstration. Soit $M\in\mathbb{K}[X]$ tel que $M\,\mathbb{K}[X]=M_0\,\mathbb{K}[X]$. Comme dans le théorème précédent, M est un multiple de M_0 et M_0 est un multiple de M et donc, il existe $\lambda\in\mathbb{K}\setminus\{0\}$ tel que $M=\lambda M_0$.

Réciproquement, si $M=\lambda M_0$, $\lambda\in\mathbb{K}\setminus\{0\}$, un multiple de M est un multiple de M_0 et donc $M\mathbb{K}[X]\subset M_0\mathbb{K}[X]$. En appliquant ce résultat au polynôme M_0 et au nombre $\frac{1}{\lambda}$, on a aussi $M_0\mathbb{K}[X]\subset M\mathbb{K}[X]$ et finalement $M\mathbb{K}[X]=M_0\mathbb{K}[X]$.

❑

Le polynôme M_0 du théorème 39 est un polynôme non nul, unitaire, multiple commun à A et B, de degré minimum. D'où la définition :

Définition 11. Soient A et B deux polynômes non nuls.

Le polynôme unitaire, multiple commun à A et B, de degré minimum, s'appelle le **PPCM unitaire** de A et B (ou plus simplement le PPCM de A et B). Il se note $A\vee B$.

Tout polynôme de la forme $\lambda(A\vee B)$, $\lambda\in\mathbb{K}\setminus\{0\}$, s'appelle **un PPCM** de A et B.

⇨ **Commentaire**.

◇ *Le théorème 39 se réénonce explicitement sous la forme* $A\mathbb{K}[X]\cap B\mathbb{K}[X]=(A\vee B)\mathbb{K}[X]$ *ou encore*

les multiples communs à deux polynômes non nuls sont les multiples de leur PPCM.

◇ *Si* $A=0$ *ou* $B=0$, *un multiple commun à* A *et* B *est un multiple de* 0 *et est donc égal à* 0. *Ainsi, si* $A=0$ *ou* $B=0$, $A\mathbb{K}[X]\cap B\mathbb{K}[X]=\{0\}$. *Dans ce cas, on peut poser* $A\vee B=0$.

2.4.2 Propriétés du PPCM de deux polynômes

On donne sans démonstration les propriétés usuelles du PPCM.

Théorème 41.

- $\forall A\in\mathbb{K}[X]\setminus\{0\}$, $A\vee A=\dfrac{1}{\text{dom}(A)}A$.
- $\forall A\in\mathbb{K}[X]\setminus\{0\}$, $A\vee 1=\dfrac{1}{\text{dom}(A)}A$.

Théorème 42.

- $\forall(A,B)\in(\mathbb{K}[X]\setminus\{0\})^2$, $A\vee B=B\vee A$.
- $\forall(A,B,C)\in(\mathbb{K}[X]\setminus\{0\})^3$, $(A\vee B)\vee C=A\vee(B\vee C)$.

Théorème 43. $\forall(A,B,C)\in(\mathbb{K}[X]\setminus\{0\})^3$, C unitaire, $(CA)\vee(CB)=C(A\vee B)$.

2.5 Polynômes premiers entre eux. Théorèmes de Bézout et Gauss

2.5.1 Polynômes premiers entre eux

On commence par le cas de deux polynômes

Définition 12. Soient A et B deux polynômes non nuls. A et B sont **premiers entre eux** si et seulement si $A\wedge B=1$.

Exemple. Soient a et b deux éléments distincts de $\mathbb{K}$. Un diviseur commun à $A = X - a$ et $B = X - b$ divise encore $\frac{1}{b-a}(A-B) = 1$ et est donc de degré 0. En particulier, $(X-a) \wedge (X-b) = 1$. Les polynômes $X-a$ et $X-b$ sont premiers entre eux.

DÉFINITION 13. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

$A_1, \ldots, A_n$ sont **premiers entre eux** si et seulement si $A_1 \wedge \ldots \wedge A_n = 1$ (on dit aussi premiers entre eux dans leur ensemble).

$A_1, \ldots, A_n$ sont **deux à deux premiers entre eux** si et seulement si $\forall (i,j) \in [\![1,n]\!]^2$, $(i \neq j \Rightarrow A_i \wedge A_j = 1)$.

Théorème 44. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

Si $A_1, \ldots, A_n$ sont deux à deux premiers entre eux, alors $A_1, \ldots, A_n$ sont premiers entre eux.

DÉMONSTRATION. Supposons $A_1, \ldots, A_n$ sont deux à deux premiers entre eux. Un diviseur unitaire commun à $A_1, \ldots, A_n$, est en particulier un diviseur unitaire commun à A_1 et à A_2 et est donc égal à 1. Ceci montre que $A_1 \wedge \ldots \wedge A_n = 1$.

❑

La réciproque de l'implication précédente est fausse. Considérons les polynômes $A = (X-1)(X-2)$, $B = (X-1)(X-3)$ et $C = (X-2)(X-3)$. $A \wedge B = (X-1)[(X-2) \wedge (X-3)] = X - 1 \neq 1$ et de même $A \wedge C = X-2$ et $B \wedge C = X-3$. Les polynômes A, B et C ne sont pas deux à deux premiers entre eux. Maintenant, en posant $D = A \wedge B \wedge C$, on a $D = (A \wedge B) \wedge C = (X-1) \wedge (X-2)(X-3)$. En particulier, D est un diviseur unitaire de $X-1$ et donc $D = X-1$ ou $D = 1$. Ensuite, $(X-2)(X-3) = X^2 - 5X + 6 = (X-4)(X-1) + 2$ et donc $X-1$ ne divise pas $(X-2)(X-3)$. Il ne reste que $D = 1$ et donc A, B et C sont premiers entre eux (nous découvrirons plus loin que des polynômes sont premiers entre eux si et seulement si ils sont sans racine commune dans $\mathbb{C}$ ce qui rendra immédiat le fait que $A \wedge B \wedge C = 1$).

2.5.2 Théorème de Bézout

On commence par le cas de deux polynômes.

Théorème 45 (théorème de Bézout). Soient A et B deux polynômes non nuls.

A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que $AU + BV = 1$.

DÉMONSTRATION. Soient A et B deux polynômes non nuls. Posons $D = A \wedge B$.

Si $D = 1$, d'après le théorème 31, il existe deux polynômes U et V tels que $AU + BV = 1$.

Réciproquement, supposons qu'il existe deux polynômes U et V tels que $AU + BV = 1$. D'après le théorème 23, un diviseur unitaire commun à A et B divise encore $AU + BV = 1$. Ceci montre que $D = 1$.

❑

Exemple. Soient a et b deux nombres distincts puis $A = X - a$ et $B = X - b$. On a $\frac{1}{b-a}(A - B) = 1$ et donc les polynômes $U = \frac{1}{b-a}$ et $V = -\frac{1}{b-a}$ sont deux polynômes tels que $AU + BV = 1$. D'après le théorème de Bézout, $A \wedge B = 1$. ❑

Exercice 5. Soit $n \in \mathbb{N}^*$.

Déterminer deux polynômes U_n et V_n tels que $X^n U + (1-X)^n V = 1$ et $\deg(U) < n$ et $\deg(V) < n$.

Solution 5. D'après la formule du binôme de Newton,

$$\begin{aligned} 1 &= (X + 1 - X)^{2n-1} \\ &= \sum_{k=0}^{2n-1} \binom{2n-1}{k} X^k (1-X)^{2n-1-k} = \sum_{k=0}^{n-1} \binom{2n-1}{k} X^k (1-X)^{2n-1-k} + \sum_{k=n}^{2n-1} \binom{2n-1}{k} X^k (1-X)^{2n-1-k} \\ &= X^n \sum_{k=n}^{2n-1} \binom{2n-1}{k} X^{k-n} (1-X)^{2n-1-k} + (1-X)^n \sum_{k=0}^{n-1} \binom{2n-1}{k} X^k (1-X)^{n-1-k}. \end{aligned}$$

Posons $U = \sum_{k=n}^{2n-1} \binom{2n-1}{k} X^{k-n} (1-X)^{2n-1-k}$ et $V = \sum_{k=0}^{n-1} \binom{2n-1}{k} X^k (1-X)^{n-1-k}$.

Déjà, pour tout $k \in [\![n, 2n-1]\!]$, $k-n \geqslant 0$ et $2n-1-k \geqslant 0$. Donc, $U \in \mathbb{K}[X]$. De même, pour tout $k \in [\![0, n-1]\!]$, $k \geqslant 0$ et $n-1-k \geqslant 0$. Donc, $V \in \mathbb{K}[X]$. Ainsi, U et V sont deux polynômes tels que $X^n U + (1-X)^n V = 1$.

Ensuite, pour tout $k \in [\![n, 2n-1]\!]$, $\deg\left(X^{k-n}(1-X)^{2n-1-k}\right) = k-n+2n-1-k = n-1$ et donc $\deg(U) \leqslant n-1 < n$. De même, pour tout $k \in [\![0, n-1]\!]$, $\deg\left(X^k(1-X)^{n-1-k}\right) = k+n-1-k = n-1$ et donc $\deg(V) \leqslant n-1 < n$.

Les polynômes $U = \sum_{k=n}^{2n-1} \binom{2n-1}{k} X^{k-n}(1-X)^{2n-1-k}$ et $V = \sum_{k=0}^{n-1} \binom{2n-1}{k} X^k(1-X)^{n-1-k}$ conviennent.

On précisera plus loin le théorème 45 : on montrera que si $\deg(A) \geqslant 1$ et $\deg(B) \geqslant 1$, on peut imposer au couple (U, V) la condition supplémentaire $\deg(U) < \deg(B)$ et $\deg(V) < \deg(A)$ et qu'un tel couple (U, V) est unique.

On passe maintenant au cas de n polynômes :

Théorème 46. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, n polynômes non nuls.

$A_1, \ldots, A_n$, sont premiers entre eux si et seulement si il existe $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que $A_1U_1 + \ldots + A_nU_n = 1$.

Démonstration. Si $A_1 \wedge \ldots \wedge A_n = 1$, alors il existe $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que $A_1U_1 + \ldots + A_nU_n = 1$ d'après le théorème 38.

Si il existe $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que $A_1U_1 + \ldots + A_nU_n = 1$, un diviseur unitaire commun à $A_1, \ldots, A_n$, est encore un diviseur unitaire de $A_1U_1 + \ldots + A_nU_n = 1$. On en déduit que $A_1 \wedge \ldots \wedge A_n = 1$.

❑

2.5.3 Théorème de Gauss

Théorème 47 (théorème de Gauss). Soient A, B et C trois polynômes non nuls.

Si A divise BC et A et B sont premiers entre eux, alors A divise C.

Démonstration. Soient A, B et C trois polynômes non nuls, tels que A divise BC et A et B soient premiers entre eux.
Il existe $Q \in \mathbb{K}[X]$ tel que $BC = QA$ et il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$. On multiple les deux membres de la dernière égalité par C et on obtient

$$C = ACU + BCV = ACU + QAV = A(CU + QV)$$

avec $CU + QV \in \mathbb{K}[X]$. Donc, A divise C.

❑

2.5.4 Quelques conséquences des théorèmes de Bézout et Gauss

On commence par fournir une amélioration du théorème de Bézout dans la situation où A et B ne sont pas des polynômes constants.

Théorème 48. Soient A et B deux polynômes de degré au moins égal à 1 et premiers entre eux.

1) Il existe un couple $(U_0, V_0) \in \mathbb{K}[X]^2$ et un seul tel que $AU_0 + BV_0 = 1$ et $\deg(U_0) < \deg(B)$ et $\deg(V_0) < \deg(A)$.

2) Les couples $(U, V) \in \mathbb{K}[X]^2$ tels que $AU + BV = 1$ sont les couples de la forme $(U_0 + QB, V_0 - QA)$ où $Q \in \mathbb{K}[X]$.

Démonstration. Soient A et B deux polynômes non nuls et premiers entre eux.

Existence. D'après le théorème de Bézout, il existe un couple $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$. La division euclidienne de U par B s'écrit $U = U_0 + Q_0B$ où U_0 et Q_0 sont deux polynômes tels que $\deg(U_0) < \deg(B)$.
On a alors $1 = AU + BV = A(U_0 + Q_0B) + BV = AU_0 + B(AQ_0 + V)$. Posons $V_0 = AQ_0 + V$ de sorte que l'on a déjà $AU_0 + BV_0 = 1$ et $\deg(U_0) < \deg(B)$.

On note que $U_0 \neq 0$ car sinon $BV_0 = 1$ ce qui est impossible car $\deg(B) \geqslant 1$ (les inversibles de l'anneau $(\mathbb{K}[X], +, \times)$ sont les constantes non nulles). Donc,

$$\begin{aligned}\deg(B) + \deg(V_0) &= \deg(BV_0) = \deg(1 - AU_0)\\ &= \deg(AU_0) \ (\text{car } \deg(AU_0) \geqslant \deg(A) \geqslant 1)\\ &= \deg(A) + \deg(U_0)\\ &< \deg(A) + \deg(B)\end{aligned}$$

puis, après simplification par l'entier $\deg(B)$, on obtient $\deg(V_0) < \deg(A)$. Ceci montre l'existence du couple (U_0, V_0).

Unicité. Soit $(U_0, V_0, U_1, V_1) \in \mathbb{K}[X]^4$ tel que $AU_0 + BV_0 = 1 = AU_1 + BV_1$ et $\deg(U_0) < \deg(B)$, $\deg(U_1) < \deg(B)$, $\deg(V_0) < \deg(A)$ et $\deg(V_1) < \deg(A)$.
On a donc $A(U_0 - U_1) = B(V_1 - V_0)$. Le polynôme B divise le polynôme $A(U_0 - U_1)$ et le polynôme B est premier au polynôme A (d'après le théorème de Bézout). D'après le théorème de Gauss, le polynôme B divise le polynôme $U_0 - U_1$. Puisque d'autre part, $\deg(U_0 - U_1) \leqslant \text{Max}\{\deg(U_0), \deg(U_1)\} < \deg(B)$, ceci impose $U_0 - U_1 = 0$ et donc aussi $V_1 - V_0 = 0$. On a montré l'unicité du couple (U_0, V_0).

Déterminons maintenant tous les couples (U, V) de polynômes vérifiant $AU + BV = 1$ (résolution de l'équation de Bézout). Soit $(U, V) \in \mathbb{K}[X]^2$.

$$\begin{aligned} AU + BV = 1 &\Leftrightarrow AU + BV = AU_0 + BV_0 \Leftrightarrow A(U - U_0) = B(V_0 - V) \\ &\Rightarrow B | A(U - U_0) \text{ et } A | B(V_0 - V) \\ &\Rightarrow B | (U - U_0) \text{ et } A | (V_0 - V) \text{ (d'après le théorème de Gauss)} \\ &\Rightarrow \exists (Q_1, Q_2) \in \mathbb{K}[X]^2 / \ U - U_0 = Q_1 B \text{ et } V_0 - V = Q_2 A \\ &\Rightarrow \exists (Q_1, Q_2) \in \mathbb{K}[X]^2 / \ U = U_0 + Q_1 B \text{ et } V = V_0 - Q_2 A. \end{aligned}$$

Réciproquement, soient $(Q_1, Q_2) \in \mathbb{K}[X]^2$ puis $U = U_0 + Q_1 B$ et $V = V_0 - Q_2 A$.

$$\begin{aligned} AU + BV = 1 &\Leftrightarrow A(U_0 + Q_1 B) + B(V_0 - Q_2 A) = 1 \Leftrightarrow AU_0 + BV_0 + AB(Q_1 - Q_2) = 1 \\ &\Leftrightarrow AB(Q_1 - Q_2) = 0 \Leftrightarrow Q_1 - Q_2 = 0 \\ &\Leftrightarrow Q_1 = Q_2. \end{aligned}$$

Les couples (U, V) solutions sont donc les couples de la forme $(U_0 + QB, V_0 - QA)$, $Q \in \mathbb{K}[X]$.

❑

Théorème 49. Soient A et B deux polynômes non nuls et unitaires. Soient $D = A \wedge B$ et $M = A \vee B$. Alors

$$MD = AB.$$

En particulier, si $A \wedge B = 1$ (et A et B unitaires), alors $A \vee B = AB$.

Démonstration. D'après le théorème 36, on peut écrire $A = DA_1$ et $B = DB_1$ où A_1 et B_1 sont deux polynômes premiers entre eux. On a alors $AB = D(DA_1B_1)$. On va vérifier que $M = DA_1B_1$.

$DA_1B_1 = AB_1 = A_1B$. Donc, DA_1B_1 est un multiple commun à A et B et par suite, DA_1B_1 est un multiple de M.

Inversement, M est un multiple commun à A et B et donc Il existe des polynômes S et T tels que $M = SA = SDA_1$ et $M = TB = TDB_1$. Puisque $D \neq 0$, on obtient après simplification $SA_1 = TB_1$. Ainsi, B_1 divise SA_1 et $B_1 \wedge A_1 = 1$. D'après le théorème de Gauss, B_1 divise S puis il existe $Q \in \mathbb{K}[X]$ tel que $S = QB_1$. On obtient $M = QDA_1B_1$ et donc M est un multiple de DA_1B_1.

En résumé, DA_1B_1 divise M et M divise DA_1B_1. Donc, il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $M = \lambda DA_1B_1$ puis $MD = \lambda D^2 A_1B_1 = \lambda AB$. Enfin, AB et MD sont des polynômes unitaires et donc

$$1 = \text{dom}(MD) = \lambda \text{dom}(AB) = \lambda.$$

Finalement, $MD = AB$.

❑

Exemple. Soient $A = (X-1)(X-2)$ et $B = (X-1)(X-3)$. $A \wedge B = (X-1)[(X-2) \wedge (X-3)] = X-1$. L'égalité $MD = AB$ s'écrit plus explicitement $(X-1)M = (X-1)^2(X-2)(X-3)$ et après simplification par le polynôme non nul $X-1$, on obtient $(X-1)(X-2) \wedge (X-1)(X-3) = (X-1)(X-2)(X-3)$. ❑

Théorème 50. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, B, $n+1$ polynômes non nuls.
$$(\forall i \in [\![1, n]\!], \ B \wedge A_i = 1) \Leftrightarrow B \wedge \left(\prod_{i=1}^{n} A_i \right) = 1.$$

Démonstration.

• Supposons que $\forall i \in [\![1, n]\!]$, $B \wedge A_i = 1$. Alors, d'après le théorème de Bézout, pour chaque $i \in [\![1, n]\!]$, il existe $(U_i, V_i) \in \mathbb{K}[X]^2$ tel que $A_iU_i + BV_i = 1$. On multiplie membre à membre ces n égalités puis on développe et on obtient une égalité de la forme $\left(\prod_{i=1}^{n} A_i \right) U + BV = 1$ où U et V sont deux polynômes. D'après le théorème de Bézout, $\left(\prod_{i=1}^{n} A_i \right) \wedge B = 1$.

• Supposons que $\left(\prod_{i=1}^{n} A_i\right) \wedge B = 1$. Il existe deux polynômes U et V tels que $\left(\prod_{j=1}^{n} A_j\right) U + BV = 1$. Mais alors, pour chaque $i \in [\![1, n]\!]$, on peut écrire

$$A_i \left(U \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} A_j \right) + BV = 1$$

et donc, pour chaque $i \in [\![1, n]\!]$, $A_i \wedge B = 1$.

❑

Un corollaire immédiat au théorème 50 est :

Théorème 51. Soient A et B deux polynômes non nuls. $(A \wedge B = 1) \Leftrightarrow \forall (n, m) \in \mathbb{N}^2$, $A^n \wedge B^m = 1$.

Théorème 52. Soient $n \geqslant 2$ puis $A_1, \ldots, A_n$, B, $n+1$ polynômes non nuls.

Si pour tout $i \in [\![1, n]\!]$, A_i divise B et si les A_i, $1 \leqslant i \leqslant n$, sont deux à deux premiers entre eux, alors $\prod_{i=1}^{n} A_i$ divise B.

Démonstration. On montre le résultat par récurrence sur n.

• Soient A_1, A_2 et B trois polynômes non nuls tels que A_1 divise B, A_2 divise B et $A_1 \wedge A_2 = 1$.
Il existe un polynôme Q tel que $B = QA_1$. Le polynôme A_2 divise QA_1 et $A_1 \wedge A_2 = 1$. D'après le théorème de Gauss, A_2 divise Q. Donc, il existe un polynôme S tel que $Q = SA_2$ puis $B = SA_1A_2$. Par suite, A_1A_2 divise B.
Le théorème est vrai quand $n = 2$.

• Soit $n \geqslant 2$. Supposons le résultat acquis pour n. Soient $A_1, \ldots, A_n, A_{n+1}$, B, $n+2$ polynômes non nuls tels que pour tout $i \in [\![1, n+1]\!]$, A_i divise B et tels que les A_i, $1 \leqslant i \leqslant n+1$, soient deux à deux premiers entre eux.

Par hypothèse de récurrence, $\prod_{i=1}^{n} A_i$ divise B et d'autre part, d'après le théorème 50, $\prod_{i=1}^{n} A_i$ et A_{n+1} sont premiers entre eux.

D'après le cas $n = 2$, B est divisible par $\left(\prod_{i=1}^{n} B_i\right) \times B_{n+1} = \prod_{i=1}^{n+1} B_i$.

Le résultat est démontré par récurrence.

❑

3 Fonctions polynômes

On va maintenant « évaluer » des polynômes en des nombres ou encore nous allons nous préoccuper de l'**aspect fonctionnel** des polynômes. Nous nous rendrons compte le moment venu que les deux aspects (formel et fonctionnel) peuvent être identifiés ou encore, à terme, nous ne ferons plus de différence entre les expressions « polynôme » et « fonction polynôme ». Dit autrement, nous établirons que deux polynômes qui prennent la même valeur en chaque x, ont obligatoirement les mêmes coefficients et en particulier qu'un polynôme qui s'annule en chaque x, a tous ses coefficients nuls.

Cette dernière phrase a l'air d'une évidence et n'en est pas du tout une. D'abord, par ce qu'une somme de terme à le droit d'être égale à 0 sans que tous ses termes ne soient égaux à 0. Mais c'est un problème plus compliqué que ça et pour l'appréhender, nous sommes obligé de faire un détour par le programme de maths spé pour comprendre qu'à plus haut niveau, les notions de polynômes formels et polynômes fonctionnels peuvent être bien distinctes.

On découvre en maths spé l'ensemble noté $\mathbb{Z}/n\mathbb{Z}$ qui est l'ensemble des n classes d'équivalence de la relation de congruence modulo n. On découvre encore, après avoir défini une addition et une multiplication, que quand p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps commutatif.
Le petit théorème de Fermat qui dans $\mathbb{Z}$ s'écrit : pour tout p premier, pour tout $a\mathbb{Z}$, $a^p \equiv a\ [p]$, s'écrira en maths spé sous la forme : $\forall x \in \mathbb{Z}/p\mathbb{Z}$, $x^p - x = 0$.
Considérons alors le polynôme $P = X^p - X$. Ce polynôme n'est pas le polynôme nul car la suite de ses coefficients est $(-1, 0, \ldots, 0, 1, 0, 0, \ldots)$. Pourtant, ce polynôme prend la valeur 0 en chaque x ou encore la fonction $x \mapsto P(x)$ est la fonction nulle. Il y a bien un problème dans le cas où $\mathbb{K}$ est un corps quelconque. Ce ne sera par contre pas le cas si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

3.1 Définition

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. La **fonction polynôme** associée au polynôme P est la fonction que l'on note (momentanément) $\widetilde{P}$ et qui est définie par :

$$\forall x \in \mathbb{K},\ \widetilde{P}(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Il est clair que pour tout $(P, Q) \in \mathbb{K}[X]^2$ et tout $\lambda \in \mathbb{K}$,

- $P = Q \Rightarrow \widetilde{P} = \widetilde{Q}$,
- $\widetilde{(P+Q)} = \widetilde{P} + \widetilde{Q}$,
- $\widetilde{(\lambda P)} = \lambda \widetilde{P}$,
- $\widetilde{(P \times Q)} = \widetilde{P} \times \widetilde{Q}$.

Mais par contre, rien ne dit que : $\widetilde{P} = \widetilde{Q} \Rightarrow P = Q$.

3.2 Racines d'un polynôme

DÉFINITION 14. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

On dit que a est **racine** de P si et seulement si $\widetilde{P}(a) = 0$.

⇨ **Commentaire** . *La définition ci-dessus fait référence à un corps $\mathbb{K}$ qui peut être ambigü. Considérons par exemple, le polynôme $P = X^2 + 1$. Puisque qu'un réel est un nombre complexe particulier, le polynôme P peut être pensé comme un élément de $\mathbb{R}[X]$ ou comme un élément de $\mathbb{C}[X]$. Si on pense le polynôme P comme un élément de $\mathbb{R}[X]$, alors le polynôme P n'a pas de racine et si on pense le polynôme P comme un élément de $\mathbb{C}[X]$, alors le polynôme P admet deux racines à savoir les nombres i et $-i$. Le plus simple pour être clair est de faire des phrases explicites : le polynôme P n'a pas de racine dans $\mathbb{R}$ ou le polynôme P a deux racines dans $\mathbb{C}$. On doit noter que le fait que les coefficients de P soient des réels (qui sont des complexes particuliers), n'empêche absolument pas d'évaluer ce polynôme en un nombre complexe non réel : $P(i) = i^2 + 1 = 0$.*

Un résultat fondamental est :

Théorème 53. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

a est racine de P si et seulement si P est divisible par $X - a$.

DÉMONSTRATION . Le polynôme $X - a$ n'est pas nul. La division euclidienne de P par $X - a$ s'écrit $P = (X - a)Q + R$ où Q et R sont deux polynômes tels que $\deg(R) \leqslant 0$. R est donc un polynôme contant que l'on note λ.
En évaluant en a les deux membres de l'égalité $P = (X - a)Q + R$, on obtient $\lambda = \widetilde{P}(a)$. Ainsi,

$$a \text{ racine de } P \Leftrightarrow \widetilde{P}(a) = 0 \Leftrightarrow R = 0 \Leftrightarrow X - a \text{ divise } P.$$

❑

Remarque. On peut proposer une autre démonstration, présentant son propre intérêt, du fait que si a est racine de P, alors P est divisible par $X - a$. Posons $P = \sum_{k=0}^{n} \alpha_k X^k$ et supposons que $P(a) = 0$. Alors,

$$P = P - P(a) = \sum_{k=0}^{n} \alpha_k X^k - \sum_{k=0}^{n} \alpha_k a^k = \sum_{k=1}^{n} \alpha_k \left(X^k - a^k\right)$$
$$= (X - a) \sum_{k=1}^{n} \alpha_k \left(X^{k-1} + aX^{k-2} + \ldots + a^{k-2}X + a^{k-1}\right).$$

Le mérite de cette démonstration est de proposer une factorisation explicite. ❑

Dans la pratique, on n'agît pas ainsi. Considérons par exemple le polynôme $P = X^3 - 13X^2 + 6X + 6$. Le nombre 1 est racine de P (car la somme des coefficients de P est nulle). Le polynôme P est donc divisible par $X - 1$, le quotient Q de la division de P par $X - 1$ étant de degré 2. Deux coefficients du quotient sont immédiats, le coefficient dominant et le coefficient constant : $X^3 - 13X^2 + 6X + 6 = (X - 1)\left(X^2 + aX - 6\right)$. Le coefficient de X dans Q s'obtient en analysant par exemple le coefficient de X^2 dans P : $a - 1 = -13$ et donc $a = -12$. Finalement,

$$X^3 - 13X^2 + 6X + 6 = (X - 1)\left(X^2 - 12X - 6\right).$$

On peut aussi poser la division de $X^3 - 13X^2 + 6X + 6$ par $X - 1$:

$$\begin{array}{r|l} X^3-13X^2+6X+6 & X-1 \\ \cline{2-2} -12X^2+6X+6 & X^2-12X-6 \\ -6X+6 & \\ 0 & \end{array}$$

Si on veut commencer à factoriser un polynôme, un problème est d'en obtenir au moins une racine. L'exercice suivant fournit un procédé pour découvrir des racines rationnelles d'un polynôme à coefficients entiers.

Exercice 6. Soit $P=\sum_{k=0}^{n} a_k X^k$, $n \geqslant 1$, un polynôme à coefficients entiers relatifs avec $a_n \neq 0$ et $a_0 \neq 0$. Soient $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ tel que $p \wedge q = 1$ puis $r = \frac{p}{q}$.

Montrer que si r est racine du polynôme P, alors p divise a_0 et q divise a_n.

Solution 6. Si $P(r)=0$, alors $a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\frac{p}{q} + a_0 = 0$ puis, après multiplication des deux membres par q^n, $a_n p^n + a^{n-1}p^{n-1}q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$.

On en déduit que $a_n p^n = -\left(a^{n-1}qp^{n-1} + \ldots + a_1 p q^{n-1} + a_0 q^n\right) = -q\left(a^{n-1}p^{n-1} + \ldots + a_1 p q^{n-2} + a_0 q^{n-1}\right)$ est un entier divisible par q. Ainsi, q divise $a_n p^n$ et $q \wedge p^n = 1$ (car $p \wedge q = 1$). D'après le théorème de Gauss, q divise a_n. De même, à partir de l'égalité $a_0 q^n = -p\left(a_n p^{n-1} + a^{n-1}qp^{n-2} + \ldots + a_1 q^{n-1}\right)$, on montre que p divise a_0.

Exemple. Considérons le polynôme $P = 2X^3+3X^2+3X+1$. Si $r = \frac{p}{q}$ est une racine rationnelle de P (avec $(p,q) \in \mathbb{Z}^* \times \mathbb{N}^*$ et $p \wedge q = 1$), alors p divise 1 et q divise 2. Donc, $p \in \{-1,1\}$ et $q \in \{1,2\}$ puis $r \in \left\{1,-1,\frac{1}{2},-\frac{1}{2}\right\}$. La calcul donne $P(1) \neq 0$, $P(-1) \neq 0$, $P\left(\frac{1}{2}\right) \neq 0$ et au dernier moment, $P\left(-\frac{1}{2}\right) = 0$. Le polynôme P est donc divisible par $X+\frac{1}{2}$ ou aussi par $2X+1$. Une factorisation explicite est

$$2X^3+3X^2+3X+1 = (2X+1)\left(X^2+X+1\right).$$

Considérons encore le polynôme $P = X^5+X+1$. Avec les notations précédentes, nécessairement $p = \pm 1$ et $q = 1$ puis $r \in \{-1,1\}$. Mais $P(1) = 3 \neq 0$ et $P(-1) = -1 \neq 0$. Le polynôme X^5+X+1 n'a donc pas de racine rationnelle (une étude brève de la fonction $x \mapsto x^5+x+1$ montre que le polynôme P a une racine réelle dans l'intervalle $[-1,0]$). ❑

Une conséquence très importante du théorème 53 est :

Théorème 54.

1) Un polynôme de degré $n \in \mathbb{N}$ a au plus n racines.

2) a) Un polynôme de degré inférieur ou égal à $n \in \mathbb{N}$ qui a au moins $n+1$ racines deux à deux distinctes est le polynôme nul.
b) Deux polynômes de degré inférieur ou égal à $n \in \mathbb{N}$ qui coïncident en au moins $n+1$ valeurs deux distinctes (c'est-à-dire tels que $\widetilde{P}$ et $\widetilde{Q}$ prennent la même valeur en au moins $n+1$ valeurs deux à deux distinctes de la variable) sont égaux.
3) a) Un polynôme qui a une infinité de racines deux à deux distinctes est le polynôme nul.
b) Deux polynômes qui coïncident en une infinité de valeurs deux distinctes sont égaux.

Démonstration .

1) Montrons le résultat par récurrence sur n.

• Un polynôme de degré 0 est une constante non nulle et donc un polynôme de degré 0 n'a pas de racine. L'affirmation est vraie quand $n = 0$.

• Soit $n \geqslant 0$. Supposons qu'un polynôme de degré $n \in \mathbb{N}$ ait au plus n racines.
Soit P un polynôme de degré $n+1$. Si P n'a pas de racine, alors P a au plus $n+1$ racines. Sinon, P a au moins une racine a. D'après le théorème 53, il existe un polynôme Q tel que $P = (X-a)Q$. Le polynôme Q est de degré n et a donc, par hypothèse de récurrence, au plus n racines. Mais alors, le polynôme P a au plus $n+1$ racines.

Le résultat est démontré par récurrence.

2) a) Si P est un polynôme de degré inférieur ou égal à n, non nul, alors P a au plus n racines d'après 1). Par contraposition, si P est un polynôme de degré inférieur ou égal à n qui a au moins $n+1$ racines deux à deux distinctes, alors $P=0$.

b) Si P et Q sont deux polynômes de degré au plus n qui coïncident en au moins $n+1$ valeurs deux à deux distinctes, alors $P-Q$ est un polynôme de degré au plus n qui a au moins $n+1$ racines deux à deux distinctes. Donc, $P-Q=0$ puis $P=Q$.

3) a) En particulier, un polynôme non nul a un nombre fini de racines deux distinctes. Par contraposition, si P a une infinité de racines, alors $P=0$.

b) Si P et Q coïncident en une infinité de valeurs, alors $P-Q$ a une infinité de racines et donc $P-Q=0$.

❑

Au passage, nous avons presque établi que :

Théorème 55. Soit P un polynôme de degré $n \in \mathbb{N}^*$. Soient $p \in [\![1,n]\!]$ puis $a_1, \ldots, a_p$, p nombres deux à deux distincts.

P admet $a_1, \ldots, a_p$ pour racines si et seulement si P est divisible par $(X-a_1)\times\ldots\times(X-a_p)$.

Ce résultat se démontre immédiatement par récurrence.

Une autre conséquence importante du théorème 54 est :

Théorème 56. $\forall (P,Q)\in\mathbb{K}[X]^2,\ \widetilde{P}=\widetilde{Q}\Leftrightarrow P=Q$.

On rappelle que deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Démonstration. On sait déjà que si $P=Q$, alors $\widetilde{P}=\widetilde{Q}$.
Réciproquement, supposons que $\widetilde{P}=\widetilde{Q}$ ou encore que pour tout $x\in\mathbb{K}$, $\widetilde{P}(x)=\widetilde{Q}(x)$. Puisque $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, $\mathbb{K}$ **est infini**. Mais alors, $\widetilde{P}$ et $\widetilde{Q}$ coïncident en une infinité de valeurs et donc $P=Q$.

❑

Il y a donc « identité entre polynôme formel et polynôme fonctionnel ». On peut identifier les deux notions (polynôme et fonction polynôme) et en particulier laisser tomber la notation $\widetilde{P}$. C'est ce que nous ferons dorénavant.

Exercice 7. Soient $n\in\mathbb{N}$ et $\theta\in\mathbb{R}$. Déterminer le reste de la division euclidienne de $(X\sin\theta+\cos\theta)^n$ par X^2+1.

Solution 7. La division euclidienne (dans $\mathbb{R}[X]$) de $P_n=(X\sin\theta+\cos\theta)^n$ par X^2+1 s'écrit

$$(X\sin\theta+\cos\theta)^n=\left(X^2+1\right)Q_n+a_nX+b_n\quad(*)$$

où $Q_n\in\mathbb{R}[X]$ et $(a_n,b_n)\in\mathbb{R}^2$. Puisqu'un réel est un complexe particulier, l'égalité $(*)$ donne aussi la division euclidienne de P_n par X^2+1 dans $\mathbb{C}[X]$. En évaluant les deux membres de l'égalité $(*)$ en i, on obtient

$$a_ni+b_n=(i\sin\theta+\cos\theta)^n=e^{in\theta}=\cos(n\theta)+i\sin(n\theta).$$

Par identification des parties réelles et imaginaires, on obtient $a_n=\sin(n\theta)$ et $b_n=\cos(n\theta)$.

Le reste de la division euclidienne de $(X\sin\theta+\cos\theta)^n$ par X^2+1 est $R_n=X\sin(n\theta)+\cos(n\theta)$.

3.3 Formule de Taylor

On a déjà donné la formule de Taylor-Laplace pour des fonctions de classe C^{n+1}. Cette formule s'applique en particulier aux fonctions polynômes. Néanmoins, puisque à plus haut niveau « polynôme » et « fonction polynôme » sont des notions qui ne coïncident pas nécessairement, on donne une version formelle de la formule de Taylor et on la démontre formellement.

On donne deux versions de la même formule :

Théorème 57 (formule de Taylor).

Pour tout $n \in \mathbb{N}$, pour tout polynôme P de degré au plus n et tout $a \in \mathbb{K}$,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Pour tout polynôme P et tout $a \in \mathbb{K}$,

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Démonstration. Soit $n \in \mathbb{N}$. Montrons d'abord la formule pour le polynôme $P_n = X^n$. Dans ce cas, pour $k \in [\![0, n]\!]$, $P^{(k)}(a) = \dfrac{n!}{(n-k)!}a^{n-k}$. D'après la formule du binôme de Newton,

$$P_n = (X-a+a)^n = \sum_{k=0}^{n} \binom{n}{k}(X-a)^k a^{n-k} = \sum_{k=0}^{n} \frac{1}{k!}\frac{n!}{(n-k)!}a^{n-k}(X-a)^k = \sum_{k=0}^{n} \frac{P_n^{(k)}(a)}{k!}(X-a)^k.$$

Soit alors $P = \sum_{k=0}^{n} \alpha_k X^k$ un polynôme de degré au plus n.

$$P = \sum_{k=0}^{n} \alpha_k P_k = \sum_{k=0}^{n} \alpha_k \left(\sum_{j=0}^{n} \frac{P_k^{(j)}(a)}{j!}(X-a)^j \right) = \sum_{j=0}^{n} \frac{1}{j!}\left(\sum_{k=0}^{n} \alpha_k P_k^{(j)}(a) \right)(X-a)^j = \sum_{j=0}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^j.$$

La deuxième formule est la même que la première car si P est un polynôme de degré au plus n, alors pour $k \geqslant n+1$, $P^{(k)}(a) = 0$ et donc $\sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

❑

Un cas particulier important du théorème 57 est :

Théorème 58. Pour tout $n \in \mathbb{N}$ et tout polynôme P de degré au plus n,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!}X^k.$$

Pour tout polynôme P,

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!}X^k.$$

Ainsi, si $(a_k)_{k\in\mathbb{N}}$ est la suite des coefficients de P, alors $\forall k \in \mathbb{N}$, $a_k = \dfrac{P^{(k)}(0)}{k!}$.

Ainsi, si $P = X^2 + 3X + 5$, alors $5 = P(0)$, $3 = P'(0)$ et $5 = \dfrac{P''(0)}{2}$.

3.4 Ordre de multiplicité d'une racine

Définition 15. Soient P un polynôme non nul et $a \in \mathbb{K}$. Soit $k \in \mathbb{N}$.

a est **racine de P d'ordre au moins k** si et seulement si il existe un polynôme Q tel que $P = (X-a)^k Q$.
a est **racine de P d'ordre k** si et seulement si il existe un polynôme Q tel que $P = (X-a)^k Q$ et $Q(a) \neq 0$.

Une racine d'ordre 1 de P s'appelle une **racine simple** de P.
Une racine d'ordre au moins 2 de P s'appelle une **racine multiple de** P.
Une racine d'ordre exactement 2 (resp. 3 ...) de P s'appelle une **racine double** de P (resp. **triple** ...).
Une racine d'ordre 0 de P n'est pas racine de P.

Si par exemple, si $P = 3X(X-1)^2$, 0 est racine simple de P, 1 est racine double de P et 2 est racine d'ordre 0 de P.

⇨ **Commentaire.**

◇ *Dire que a est racine d'ordre k de P, c'est dire que P est divisible par $(X-a)^k$ et pas par $(X-a)^{k+1}$.*

◇ *Il est clair que l'ordre de multiplicité d'une racine d'un polynôme non nul est inférieur ou égal à son degré.*

◇ *Nous avons défini l'ordre de multiplicité d'une racine d'un polynôme non nul. La notion d'ordre de multiplicité n'a pas de sens quand* $P = 0$ *car dans ce cas, « tout nombre est racine à tout ordre ». Par exemple,* $0 = 0 \times (X-1) = 0 \times (X-1)^2 = \dots$ *et donc* 1 *est racine du polynôme nul d'ordre au moins* 1*, au moins* 2*, ...*

On donne maintenant une caractérisation de l'ordre de multiplicité d'une racine d'un polynôme à partir des dérivées successives de ce polynôme.

Théorème 59. Soient P un polynôme non nul et $a \in \mathbb{K}$. Soit $k \in \mathbb{N}^*$.

a est racine de P d'ordre au moins égal à k si et seulement si $P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0$.
a est racine de P d'ordre exactement égal à k si et seulement si $P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

Démonstration .

• Soit P un polynôme non nul de degré $n \in \mathbb{N}^*$. Soit $k \in [\![1, n]\!]$. Soit $a \in \mathbb{K}$. La formule de Taylor fournit

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

Puisque $\deg\left(\sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i\right) < k$, $R = \sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i$ est le reste de la division euclidienne de P par $(X-a)^k$. Par suite,

$$\begin{aligned} a \text{ racine de } P \text{ d'ordre supérieur ou égal à } k &\Leftrightarrow P \text{ est divisible par } (X-a)^k \\ &\Leftrightarrow \sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i = 0. \end{aligned}$$

Montrons alors que $\sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i = 0 \Leftrightarrow \forall i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0$.

Il est clair que si $\forall i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0$, alors $\sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i = 0$.

Inversement, supposons qu'il existe $i \in [\![0, k-1]\!]$ tel que $P^{(i)}(a) \neq 0$. Soit $i_0 = \text{Max}\{i \in [\![0, k-1]\!] / \ P^{(i)}(a) \neq 0\}$. Par définition, $P^{(i_0)}(a) \neq 0$ puis $\deg\left(\sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i\right) = \deg\left(\sum_{i=0}^{i_0} \frac{P^{(i)}(a)}{i!}(X-a)^i\right) = \deg\left(\frac{P^{(i_0)}(a)}{i_0!}(X-a)^{i_0}\right) = i_0$ et en particulier, $\sum_{i=0}^{k-1} \frac{P^{(i)}(a)}{i!}(X-a)^i \neq 0$.

On a montré que : a est racine de P d'ordre supérieur ou égal à k si et seulement si $\forall i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0$.

• Maintenant, a est racine de P d'ordre exactement k si et seulement si a est racine de P d'ordre supérieur ou égal à k et n'est pas racine de P d'ordre supérieur ou égal à $k+1$. Ceci équivaut à $\forall i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0$ et $P^{(k)}(a) \neq 0$.

❑

Exemple. Considérons le polynôme $P = (X-2)^2(X-3)^2$. 2 est racine double de P. $P' = 2(X-2)(X-3)^2 + 2(X-2)^2(X-3) = 2(X-2)(X-3)(2X-5)$. Ensuite, $P'' = 2(X-3)(2X-5) + 2(X-2)((X-3)(2X-5))'$ et donc $P(2) = P'(2) = 0$ et $P''(2) \neq 0$.
❑

Quand a est racine d'ordre k de P, on sait que $P(a) = \dots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$. Mais on n'a aucun renseignement sur $P^{(k+1)}(a)$. Par exemple, si $P = X^2$, $P(0) = P'(0) = 0$, $P''(0) = 2 \neq 0$ et $P^{(3)}(0) = 0$ et si $P = X^2(X+1)$, $P(0) = P'(0) = 0$, $P''(0) = 2 \neq 0$ et $P^{(3)}(0) = 6 \neq 0$.

Du théorème 59, on déduit en particulier :

Théorème 60. Soient P un polynôme de degré $n \in \mathbb{N}^*$ admettant $a \in \mathbb{K}$ pour racine d'ordre $k \in [\![1, n]\!]$.

Alors, pour tout $l \in [\![0, k]\!]$, a est racine d'ordre $k-l$ de $P^{(l)}$.

Démonstration . Soient $l \in [\![0, k]\!]$ puis $Q = P^{(l)}$.
Si $l < k$, $Q(a) = P^{(l)}(a) = 0$, $Q'(a) = P^{(l+1)}(a) = 0$, ..., $Q^{(k-l-1)}(a) = P^{(k-1)}(a) = 0$ et $Q^{(k-l)}(a) = P^{(k)}(a) \neq 0$. Donc, a est racine d'ordre $k-l$ de $P^{(l)}$.
Si $l = k$, $Q(a) = P^{(k)}(a) \neq 0$ et donc a n'est pas racine de Q ou encore a est racine de Q d'ordre $0 = k-k$.

❑

Sinon, la notion d'ordre de multiplicité d'une racine aide à factoriser un polynôme (la factorisation complète étant analysée dans la section suivante « Factorisation en produit de facteurs irréductibles »).

Théorème 61. Soit P un polynôme non nul admettant p racines deux à deux distinctes $a_1, \dots, a_p$, d'ordres de multiplicité respectifs $\alpha_1, \dots, \alpha_p$ (qui sont des entiers naturels non nuls).

Alors, P est divisible par $(X-a_1)^{\alpha_1} \dots (X-a_k)^{\alpha_p}$.

Démonstration. Puisque les a_i, $1 \leqslant i \leqslant p$, sont deux à deux distincts, les polynômes $X-a_i$, $1 \leqslant i \leqslant p$, sont deux à deux premiers entre eux. Il en est de même des polynômes $(X-a_i)^{\alpha_i}$, $1 \leqslant i \leqslant p$, d'après le théorème 51. Chaque polynôme $(X-a_i)^{\alpha_i}$, $1 \leqslant i \leqslant p$, divise P et ces polynômes sont deux à deux premiers entre eux. Donc, $\prod_{i=1}^{p}(X-a_i)^{\alpha_i}$ divise P d'après le théorème 52.

❑

Exercice 8. Déterminer un polynôme $P \in \mathbb{R}[X]$ de degré 5 tel que $P(X)+10$ est divisible par $(X+2)^3$ et $P(X)-10$ est divisible par $(X-2)^3$.

Solution 8. Le polynôme $P(X)+10$ admet -2 pour racine d'ordre au moins égal à 3 et donc le polynôme $P' = (P(X)+10)'$ admet -2 pour racine d'ordre au moins égal à 2. De même, le polynôme P' admet 2 pour racine d'ordre au moins égal à 2.

Puisque P' est de degré 4, il existe nécessairement $\lambda \in \mathbb{R}\setminus\{0\}$ tel que

$$P' = \lambda(X-2)^2(X+2)^2 = \lambda\left(X^2-4\right)^2 = \lambda\left(X^4-8X^2+16\right),$$

Puis il existe nécessairement $(\lambda,\mu) \in (\mathbb{R}\setminus\{0\})\times\mathbb{R}$ tel que

$$P = \lambda\left(\frac{X^5}{5} - \frac{8X^3}{3} + 16X\right) + \mu.$$

Réciproquement, soit P un tel polynôme. Alors, $P' = \lambda(X-2)^2(X+2)^2$ puis $P'(2) = P''(2) = P'(-2) = P''(-2) = 0$.
Si le polynôme $P_1 = P+10$ ne s'annule pas en -2, alors $P+10$ n'est pas divisible par $(X+2)^3$ et si le polynôme P_1 s'annule en -2, alors, puisque $P_1' = P'$, $P_1(-2) = P_1'(-2) = P''(-2) = 0$ puis $P+10$ est divisible par $(X+2)^3$.
De même, $P-10$ est divisible par $(X-2)^3$ si et seulement si le polynôme $P_2 = P-10$ s'annule en 2. Finalement,

$$P \text{ solution} \Leftrightarrow \left\{\begin{array}{l} P(2) = 10 \\ P(-2) = -10 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \lambda\left(\frac{32}{5} - \frac{64}{3} + 32\right) + \mu = 10 \\ -\lambda\left(\frac{32}{5} - \frac{64}{3} + 32\right) + \mu = -10 \end{array}\right.$$

$$\Leftrightarrow\Leftrightarrow \left\{\begin{array}{l} \mu = 0 \ (I+II) \\ 32\lambda\left(\frac{1}{5} - \frac{2}{3} + 1\right) = 10 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \mu = 0 \\ \frac{32\times 8}{15}\lambda = 10 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \mu = 0 \\ \lambda = \frac{75}{128} \end{array}\right.$$

Il existe un polynôme et un seul solution à savoir le polynôme $P = \frac{75}{128}\left(\frac{X^5}{5} - \frac{8X^3}{3} + 16X\right)$.

Exercice 9. Pour $n \in \mathbb{N}^*$, on pose $P_n = \left(X^2-1\right)^n$ puis $L_n = P_n^{(n)}$.

1) Déterminer le degré et le coefficient dominant de L_n.

2) Montrer que L_n a n racines simples, toutes éléments de $]-1,1[$.

Solution 9.

1) Soit $n \in \mathbb{N}$. $\deg(P_n) = 2n$ et donc $\deg(L_n) = 2n-n = n$.

Ensuite, $\text{dom}(P_n) = 1$ et donc $\text{dom}(L_n) = (2n)(2n-1)\dots(n+1) = \frac{(2n)!}{n!}$.

2) Montrons par récurrence (finie) que pour tout $k \in [\![0,n]\!]$, $P_n^{(k)}$ admet (au moins) k racines deux à deux distinctes dans $]-1,1[$.

- Le résultat est clair pour $k=0$.
- Soit $k \in [\![0,n-1]\!]$. Supposons que $P_n^{(k)}$ s'annule en k réels deux à deux distincts de $]-1,1[$. P_n admet 1 et -1 pour

racines d'ordre n et donc $P_n^{(k)}$ admet 1 et -1 pour racine d'ordre $n-k$ avec $n-k \geqslant n-(n-1)=1$. En particulier, $P_n^{(k)}$ s'annule en 1 et en -1. Ainsi, $P_n^{(k)}$ s'annule en $k+2$ réels deux à deux distincts de $[-1,1]$. Ces $k+2$ réels découpent l'intervalle $[-1,1]$ en $k+1$ intervalles de longueur non nulle et $P_n^{(k)}$ prend la même valeur aux bornes de chacun de ces intervalles. D'après le théorème de ROLLE, $P_n^{(k+1)} = \left(P_n^{(k)}\right)'$ s'annule au moins une fois dans chacun des $k+1$ intervalles ouverts et donc s'annule en au moins $k+1$ réels deux à deux distincts de l'intervalle $]-1,1[$.

Le résultat est démontré par récurrence. En particulier, pour $k=n$, $L_n = P_n^{(n)}$ s'annule en (au moins) n réels deux à deux distincts $a_1, \ldots, a_n$, tous éléments de l'intervalle $]-1,1[$. On sait qu'il existe un polynôme Q tel que $P = Q(X-a_1)\ldots(X-a_n)$. De plus, $\deg(L_n) = n$ et donc Q est une constante non nulle. Plus précisément, puisque le polynôme $(X-a_1)\ldots(X-a_n)$ est unitaire, $Q = \mathrm{dom}(L_n) = \dfrac{(2n)!}{n!}$ et donc

$$L_n = \frac{(2n)!}{n!}(X-a_1)\ldots(X-a_n).$$

Ceci montre que L_n admet exactement n racines réelles deux à deux distinctes, toutes simples et dans $]-1,1[$.

3.5 Polynômes d'interpolation de LAGRANGE

On se donne $n+1$ nombres complexes ($n \in \mathbb{N}^*$) deux à deux distincts $a_0, \ldots, a_n$ puis $n+1$ autres nombres complexes pas nécessairement deux à deux distincts $b_0, \ldots, b_n$. On cherche un polynôme P de degré au plus n vérifiant les égalités

$$\forall i \in [\![0,n]\!],\ P(a_i) = b_i.$$

On va montrer l'existence et l'unicité d'un tel polynôme et en donner une expression.

Par exemple, le polynôme P de degré au plus 1 vérifiant $P(1)=1$ et $P(3)=-5$ est

$$P = \frac{-5-1}{3-1}(X-1)+1 = -3X+4.$$

On commence par analyser un cas très particulier du problème. Soit $i \in [\![0,n]\!]$. Montrons l'existence et l'unicité d'un polynôme L_i, de degré au plus n, vérifiant

$$\forall j \in [\![0,n]\!],\ L_i(a_j) = \delta_{i,j} = \begin{cases} 1 \text{ si } j=i \\ 0 \text{ si } j \neq i \end{cases}.$$

L_i doit s'annuler en chacun des n nombres complexes deux à deux distincts a_j, $j \in [\![0,n]\!]\backslash\{i\}$. Donc, il existe nécessairement un polynôme Q tel que $L_i = Q\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}(X-a_j)$. Puisque $\deg(L_i) \leqslant n$, on a $\deg(Q) \leqslant 0$ et donc il existe $\lambda \in \mathbb{K}$ tel que $L_i = \lambda\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}(X-a_j)$. Enfin, l'égalité $L_i(a_i)=1$ impose

$$\lambda\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}(a_i-a_j) = 1$$

et donc $\lambda = \dfrac{1}{\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}(a_i-a_j)}$. Ainsi, nécessairement, $L_i = \prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}\dfrac{X-a_j}{a_i-a_j}$. Ceci montre l'unicité de L_i.

Réciproquement, posons $L_i = \prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}}\dfrac{X-a_j}{a_i-a_j}$. Puisque les a_i sont deux à deux distincts, L_i est bien défini et est un polynôme de degré n. De plus, pour tout $j \neq i$,

$$L_i(a_j) = \prod_{\substack{0\leqslant k\leqslant n\\ k\neq i}}\frac{a_j-a_k}{a_i-a_k} = (a_j-a_j)\prod_{\substack{0\leqslant k\leqslant n\\ k\neq i,\ k\neq j}}\frac{a_j-a_k}{a_i-a_k} = 0$$

et

$$L_i(a_j) = \prod_{\substack{0\leqslant k\leqslant n\\ k\neq i}}\frac{a_i-a_k}{a_i-a_k} = 1.$$

Le polynôme L_i convient. Ceci montre l'existence de L_i. On peut énoncer :

Théorème 62. Soit $n \in \mathbb{N}^*$. Soient $a_0, \dots, a_n$, $n+1$ éléments de $\mathbb{K}$ deux à deux distincts.

Pour chaque $i \in [\![0, n]\!]$, il existe un polynôme L_i et un seul de degré inférieur ou égal à n vérifiant

$$\forall j \in [\![0, n]\!],\ L_i(a_j) = \delta_{i,j}.$$

De plus,

$$L_i = \prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}.$$

Passons maintenant au cas général. On rappelle que $a_0, \dots, a_n$, sont $n+1$ éléments de $\mathbb{K}$ deux à deux distincts, que $b_0, \dots, b_n$, sont $n+1$ nombres et que l'on cherche un polynôme P de degré inférieur ou égal à n vérifiant de plus : $\forall i \in [\![0, n]\!]$, $P(a_i) = b_i$.

• Montrons l'existence d'un tel polynôme. Soit $P = \sum_{j=0}^{n} b_j L_j$. Puisque chaque L_j, $0 \leqslant j \leqslant n$, est de degré n, P est de degré inférieur ou égal à n. D'autre part, pour $i \in [\![0, n]\!]$,

$$P(a_i) = \sum_{j=0}^{n} b_j L_j(a_i) = \sum_{j=0}^{n} b_j \delta_{i,j} = b_i.$$

Donc, le polynôme P convient.

• Montrons l'unicité d'un tel polynôme. Soient P et Q deux polynômes de degrés inférieurs ou égaux à n vérifiant pour tout $i \in [\![0, n]\!]$, $P(a_i) = b_i = Q(a_i)$. Ces deux polynômes coïncident en au moins $n+1$ valeurs deux à deux distinctes et sont de degrés au plus n. On en déduit que $P = Q$ d'après le théorème 54.

On peut énoncer :

Théorème 63. Soit $n \in \mathbb{N}^*$. Soient $a_0, \dots, a_n$, $n+1$ éléments de $\mathbb{K}$ deux à deux distincts et $b_0, \dots, b_n$, $n+1$ éléments de $\mathbb{K}$.

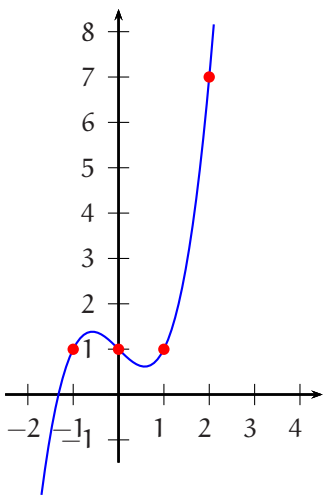
Il existe un et un seul polynôme L de degré inférieur ou égal à n tel que pour tout $i \in [\![0, n]\!]$, $L(a_i) = b_i$ à savoir

$$L = \sum_{i=0}^{n} b_i L_i = \sum_{i=0}^{n} b_i \prod_{\substack{0 \leqslant j \leqslant n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}.$$

Par exemple, le polynôme L de degré inférieur ou égal à 3 vérifiant $L(-1) = 1$, $L(0) = 1$, $L(1) = 1$ et $L(2) = 7$ est

$$\begin{aligned} L &= 1 \times \frac{(X-0)(X-1)(X-2)}{(-1-0)(-1-1)(-1-2)} + 1 \times \frac{(X+1)(X-1)(X-2)}{(0+1)(0-1)(0-2)} + 1 \times \frac{(X+1)(X-0)(X-2)}{(1+1)(1+0)(1-2)} + 7 \times \frac{(X+1)(X-0)(X-1)}{(2+1)(2-0)(2-1)} \\ &= -\frac{1}{6}X(X-1)(X-2) + \frac{1}{2}(X+1)(X-1)(X-2) - \frac{1}{2}X(X+1)(X-2) + \frac{7}{6}(X+1)X(X-1) = X^3 - X + 1. \end{aligned}$$

Voici son graphe :



4 Factorisation en produits de polynômes irréductibles

4.1 Le théorème de d'Alembert-Gauss

Nous admettrons le « théorème fondamental de l'algèbre » (on n'a pas vraiment les outils pour démontrer ce théorème avant la maths spé) :

Théorème 64 (théorème de d'Alembert-Gauss). Soit P un élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1.

P admet au moins une racine (dans $\mathbb{C}$).

Il s'agit d'une propriété du corps $(\mathbb{C}, +, \times)$: toute équation polynomiale à coefficients dans $\mathbb{C}$ de degré supérieur ou égal à 1 admet au moins une solution dans $\mathbb{C}$. De manière générale, un corps commutatif $\mathbb{K}$ vérifiant cette propriété est dit **algébriquement clos**. Une variante du théorème de d'Alembert-Gauss est donc :

Théorème 65 (théorème de d'Alembert-Gauss). $\mathbb{C}$ est algébriquement clos.

Par exemple, l'équation $z^6 + z^4 + 1 = 0$ admet au moins une solution dans $\mathbb{C}$. On note que le théorème ne fournit aucun procédé pour l'obtenir et de fait, personne au monde ne sait donner la valeur exacte d'une solution. Au degré 2, on dispose de formules fournissant les solutions en fonction des coefficients de l'équation ($\frac{-b \pm \delta}{2a}$ où $\delta^2 = b^2 - 4ac$). Une telle formule existe encore au degré 3 (formules de Cardan, formule contenant entre autres des racines carrées et des racines cubiques) et au degré 4 (formules de Ferrari). Mais il a été démontré qu'il n'est plus possible d'obtenir de telles formules pour les équations de degré supérieur ou égal à 5 : « l'équation générale de degré supérieur ou égal à 5 n'est pas résoluble par radicaux ». Ceci n'empêche pas de savoir résoudre, ponctuellement, certaines équations de degré 5 comme $z^5 - 1 = 0$ par exemple.

On peut donner une nouvelle variante du théorème fondamental de l'algèbre avec la définition suivante.

Définition 16. Soit P un élément de $\mathbb{K}[X]$ de degré supérieur ou égal à 1.

P est **scindé sur** $\mathbb{K}$ si et seulement si P est un produit de polynômes de degré 1 à coefficients dans $\mathbb{K}$.

Par exemple, le polynôme $P = 2(X-1)^2(X-2) = (2X-2)(X-1)(X-2)$ est scindé sur $\mathbb{R}$. Le polynôme X^2+1 n'est pas scindé sur $\mathbb{R}$ car dans le cas contraire, il serait produit de deux polynômes de degré 1 à coefficients réels et il admettrait une racine réelle, ce qui est faux. Par contre, le polynôme X^2+1 est scindé sur $\mathbb{C}$ car $X^2+1 = (X-i)(X+i)$. On note que la phrase « P est scindé » ne veut rien dire si on ne précise pas le corps $\mathbb{K}$.

Avec cette nouvelle notion, on peut donner une nouvelle variante du théorème 64 :

Théorème 66 (théorème de d'Alembert-Gauss). Tout élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 est scindé sur $\mathbb{C}$.

Plus précisément, tout élément de $\mathbb{C}[X]$ de degré $n \geqslant 1$, peut s'écrire sous la forme $\lambda(X-a_1)\dots(X-a_n)$ où λ est un nombre complexe non nul et $a_1, \dots, a_n$, sont des nombres complexes pas nécessairement deux à deux distincts.

Démonstration. Montrons par récurrence que pour tout $n \in \mathbb{N}^*$ et tout polynôme $P \in \mathbb{C}[X]$ de degré n, P est scindé sur $\mathbb{C}$.

- Tout élément de $\mathbb{C}[X]$ de degré 1 est produit d'un polynôme de degré 1. L'affirmation est vraie quand $n = 1$.
- Soit $n \geqslant 1$. Supposons que tout élément de $\mathbb{C}[X]$ de degré n soit scindé sur $\mathbb{C}$. Soit P un élément de $\mathbb{C}[X]$ de degré $n+1$. Puisque $n+1 \geqslant 1$, d'après le théorème 64, P admet au moins une racine a_1 dans $\mathbb{C}$ et donc, il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-a_1) \times Q$. Q est degré n et par hypothèse de récurrence, Q s'écrit sous la forme $\lambda(X-a_2)\dots(X-a_{n+1})$ où λ est un nombre complexe non nul et $a_2, \dots, a_{n+1}$, sont des nombres complexes. Mais alors,

$$P = \lambda(X-a_1)(X-a_2)\dots(X-a_{n+1}).$$

Le résultat est démontré par récurrence.

❑

4.2 Polynômes irréductibles sur un corps

Tout le cours d'arithmétique dans $\mathbb{K}[X]$ évolue en parallèle avec le cours d'arithmétique dans $\mathbb{Z}$. Ceci tient entre autres dans le fait qu'il existe dans l'anneau $(\mathbb{Z}, +, \times)$ et dans l'anneau $(\mathbb{K}[X], +, \times)$ une division euclidienne. Le théorème fondamental de l'arithmétique dans $\mathbb{Z}$ dit que tout entier n supérieur ou égal à 2 se décompose, de manière unique à l'ordre près des facteurs, en un produit de nombres premiers. La notion de nombre premier dans $\mathbb{N}^*$ a son analogue dans $\mathbb{K}[X]$: la notion de polynôme irréductible sur $\mathbb{K}$. De même que, dans $\mathbb{N}^*$, le nombre 1 ne fait pas partie de la liste des nombres premiers pour

assurer l'unicité de la décomposition, un polynôme de degré 0 ne fera pas partie de la liste des polynômes irréductibles sur $\mathbb{K}$ pour assurer l'unicité de la décomposition dans $\mathbb{K}[X]$.

DÉFINITION 17. Soit P un élément de $\mathbb{K}[X]$ de degré supérieur ou égal à 1.

P est **irréductible sur** $\mathbb{K}$ si et seulement si il n'existe pas de polynômes A et B, tous deux de degré supérieur ou égal à 1, tel que $P = AB$.

⇨ **Commentaire** .

◇ *Un polynôme de degré* 1 *est irréductible sur* $\mathbb{K}$ *par définition.*

◇ *On peut donner de nombreuses variantes de la définition d'un polynôme irréductible. En voici une :* P *est irréductible sur* $\mathbb{K}$ *si et seulement si* $\forall (A,B) \in \mathbb{K}[X]^2$, $(P = AB \Rightarrow deg(A) = 0$ *ou* $deg(B) = 0)$.

◇ *On note aussi que* P *n'est pas irréductible sur* $\mathbb{K}$ *si et seulement si il existe* $(A,B) \in \mathbb{B}[X]^2$ *tel que* $P = AB$ *et* $deg(A) \geqslant 1$ *et* $deg(B) \geqslant 1$.

◇ *Un polynôme qui n'a pas de racine dans* $\mathbb{K}$ *n'est pas nécessairement irréductible sur* $\mathbb{K}$. *Considérons par exemple le polynôme* $P = X^4 + X^2 + 1 \in \mathbb{R}[X]$. P *n'a pas de racine dans* $\mathbb{R}$ *car pour tout réel* x, $P(x) = x^4 + x^2 + 1 > 0$. *Pourtant*

$$P = X^4 + 2X^2 + 1 - X^2 = \left(X^2+1\right)^2 - X^2 = \left(X^2+X+1\right)\left(X^2-X+1\right)$$

et le polynôme P *n'est pas irréductible sur* $\mathbb{R}$.

Une nouvelle variante du théorème de d'ALEMBERT-GAUSS est :

Théorème 67 (théorème de d'ALEMBERT-GAUSS).

Les polynômes irréductibles sur $\mathbb{C}$ sont les polynômes de degré 1.

4.3 Factorisation en produits de polynômes irréductibles dans $\mathbb{C}[X]$

Théorème 68. Soit P un élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1.

P s'écrit, de manière unique à l'ordre près des facteurs, sous la forme

$$P = \lambda \prod_{k=1}^{p} (X - z_k)^{\alpha_k}$$

où $z_1, \ldots, z_p$, sont des nombres complexes deux à deux distincts et $\alpha_1, \ldots, \alpha_p$ sont des entiers naturels non nuls.

DÉMONSTRATION . L'unicité de la décomposition vient du fait que nécessairement λ est le coefficient dominant de P, les z_i sont nécessairement les racines deux à deux distinctes de P et les α_i leurs ordres de multiplicité respectifs.

Démontrons l'existence d'une telle décomposition. Soit $P \in \mathbb{C}[X]$ tel que $\deg(P) \geqslant 1$. Soient $z_1, \ldots, z_p$, les racines deux à deux distinctes de P dans $\mathbb{C}$ (on sait qu'il y en a au moins une et qu'il y en a un nombre fini) et $\alpha_1, \ldots, \alpha_p$ leurs ordres de multiplicité respectifs. Les α_i, $1 \leqslant i \leqslant p$, sont par définition des entiers naturels non nuls.

On sait d'après le théorème de BÉZOUT que les polynômes $X - z_k$, $1 \leqslant k \leqslant p$, sont deux à deux premiers entre eux. On sait qu'il en est de même des polynômes $(X - z_k)^{\alpha_k}$, $1 \leqslant k \leqslant p$. Chaque polynôme $(X - z_k)^{\alpha_k}$, $1 \leqslant k \leqslant p$, divise P et ces polynômes sont deux à deux premiers entre eux. On sait alors que P est divisible par $\prod_{k=1}^{p} (X - z_k)^{\alpha_k}$. Donc, il existe $Q \in \mathbb{K}[X] \setminus \{0\}$ tel que $P = Q \prod_{k=1}^{p} (X - z_k)^{\alpha_k}$.
Si $\deg(Q) \geqslant 1$, Q admet au moins une racine dans $\mathbb{C}$ d'après le théorème de d'ALEMBERT-GAUSS. Cette racine est encore une racine de P et donc cette racine est un certain z_{k_0}, $1 \leqslant k_0 \leqslant p$. Mais alors, Q est divisible par $X - z_{k_0}$ puis P est divisible $(X - z_{k_0})^{\alpha_{k_0}+1}$ ce qui contredit la définition de l'ordre de multiplicité.

Donc, $\deg(Q) = 0$ et on a montré qu'il existe $\lambda \in \mathbb{C} \setminus \{0\}$ tel que $P = \lambda \prod_{k=1}^{p} (X - z_k)^{\alpha_k}$.

❑

4.4 Factorisation en produits de polynômes irréductibles dans $\mathbb{R}[X]$

On va déduire la factorisation en produit de polynômes irréductibles dans $\mathbb{R}[X]$ de la factorisation déjà effectuée dans $\mathbb{C}[X]$ (puisque $\mathbb{R}[X] « \subset » \mathbb{C}[X]$). On commence par :

DÉFINITION 18. Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$.

Le **conjugué** du polynôme P est le polynôme, noté $\overline{P}$, dont les coefficients sont les conjugués des coefficients de P.
Donc, $\overline{P} = \sum_{k=0}^{+\infty} \overline{a_k} X^k$.

Il s'agit d'une « conjugaison formelle » (on a conjugué les coefficients). Les propriétés usuelles de cette conjugaison formelle sont :

Théorème 69.

1) $\forall (P,Q) \in \mathbb{C}[X]^2$, $\overline{P+Q} = \overline{P} + \overline{Q}$.
2) $\forall (P,\lambda) \in \mathbb{C}[X] \times \mathbb{C}$, $\overline{(\lambda P)} = \overline{\lambda}\overline{P}$.
3) $\forall (P,Q) \in \mathbb{C}[X]^2$, $\overline{P \times Q} = \overline{P} \times \overline{Q}$.
4) $\forall P \in \mathbb{C}[X]$, $\forall j \in \mathbb{N}$, $\overline{P^{(j)}} = \overline{P}^{(j)}$.
5) $\forall P \in \mathbb{C}[X]$, $\forall z \in \mathbb{C}$, $\overline{P(z)} = \overline{P}(\overline{z})$.
6) $\forall P \in \mathbb{C}[X]$, $\left(P \in \mathbb{R}[X] \Leftrightarrow \overline{P} = P\right)$.

DÉMONSTRATION.

1) Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux éléments de $\mathbb{C}[X]$.

$$\overline{P+Q} = \sum_{k=0}^{+\infty} \overline{a_k + b_k} X^k = \sum_{k=0}^{+\infty} \left(\overline{a_k} + \overline{b_k}\right) X^k = \sum_{k=0}^{+\infty} \overline{a_k} X^k + \sum_{k=0}^{+\infty} \overline{b_k} X^k = \overline{P} + \overline{Q}.$$

2) Soient $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$ et $\lambda \in \mathbb{C}$.

$$\overline{\lambda P} = \sum_{k=0}^{+\infty} \overline{\lambda a_k} X^k = \sum_{k=0}^{+\infty} \left(\overline{\lambda}\overline{a_k}\right) X^k = \overline{\lambda} \sum_{k=0}^{+\infty} \overline{a_k} X^k = \overline{\lambda}\overline{P}.$$

3) Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ deux éléments de $\mathbb{C}[X]$.

$$\overline{P \times Q} = \sum_{k=0}^{+\infty} \overline{\left(\sum_{i=0}^{k} a_i b_{k-i}\right)} X^k = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} \overline{a_i}\overline{b_{k-i}}\right) X^k = \overline{P} \times \overline{Q}.$$

4) Soient $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$ et $i \in \mathbb{N}$.

$$\overline{P^{(j)}} = \sum_{k=j}^{+\infty} \overline{\left(\frac{k!}{(k-j)!} a_k\right)} X^{k-j} = \sum_{k=j}^{+\infty} \frac{k!}{(k-j)!} \overline{a_k} X^{k-j} = \overline{P}^{(j)}.$$

5) Soient $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$ et $z \in \mathbb{C}$.

$$\overline{P(z)} = \overline{\sum_{k=0}^{+\infty} a_k z^k} = \sum_{k=0}^{+\infty} \overline{a_k}\, \overline{z}^k = \overline{P}(\overline{z}).$$

6) Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$.

$$P \in \mathbb{R}[X] \Leftrightarrow \forall k \in \mathbb{N},\ a_k \in \mathbb{R} \Leftrightarrow \forall k \in \mathbb{N},\ \overline{a_k} = a_k \Leftrightarrow \overline{P} = P.$$

❑

Théorème 70. Soit P un élément de $\mathbb{R}[X]$ de degré supérieur ou égal à 1. Soit $z \in \mathbb{C}$.

z est racine de P si et seulement si $\overline{z}$ est racine de P.

DÉMONSTRATION. Puisque $P \in \mathbb{R}[X]$, $\overline{P} = P$ puis pour tout $z \in \mathbb{C}$,

$$P(\overline{z}) = \overline{P}(\overline{z}) = \overline{P(z)}.$$

En particulier, pour tout $z \in \mathbb{C}$, $P(z) = 0 \Leftrightarrow P(\overline{z}) = 0$.

❑

Théorème 71. Les polynômes de $\mathbb{R}[X]$, irréductibles sur $\mathbb{R}$, sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Démonstration .

• Un élément de $\mathbb{R}[X]$ de degré 1 est irréductible sur $\mathbb{R}$.

• Soit P un élément de $\mathbb{R}[X]$ de degré 2. Si $\Delta \geqslant 0$, P admet deux racines réelles a et b pas nécessairement distinctes et s'écrit $P = \mathrm{dom}(P)(X-a)(X-b)$. Dans ce cas, P n'est pas irréductible sur $\mathbb{R}$.
Si $\Delta < 0$, P n'admet pas de racine réelle. P ne s'écrit donc pas comme un produit de deux polynômes de degré 1 à coefficients réels et donc P est irréductible sur $\mathbb{R}$.

• Soit P un élément de $\mathbb{R}[X]$ de degré supérieur ou égal à 3. D'après le théorème de d'Alembert-Gauss, P a au moins une racine a dans $\mathbb{C}$.

Si $a \in \mathbb{R}$, puisque $P \in \mathbb{R}[X]$, il existe $Q \in \mathbb{R}[X]$ tel que $P = (X-a)Q$ et $\deg(Q) \geqslant 3-1 = 2$. Dans ce cas, P n'est pas irréductible.

Si $a \notin \mathbb{R}$, $\overline{a}$ est aussi racine de P (avec $\overline{a} \neq a$) d'après le théorème précédent et donc P est divisible par $(X-a)(X-\overline{a}) = X^2 - 2X\mathrm{Re}(a) + |a|^2 \in \mathbb{R}[X]$. Donc, il existe $Q \in \mathbb{R}[X]$ tel que $P = \left(X^2 - 2X\mathrm{Re}(a) + |a|^2\right) Q$ et $\deg(Q) \geqslant 3-2 = 1$. Dans ce cas, P n'est pas irréductible.

En résumé, tout polynôme à coefficients réels de degré supérieur ou égal à 3, n'est pas irréductible sur $\mathbb{R}$.

❑

⇨ **Commentaire** . *Si P est de degré 2 à coefficients réels, les phrases « P est irréductible sur $\mathbb{R}$ » et « P n'a pas de racine réelle » sont équivalentes. Ce résultat est faux dans le cas général. On a par exemple constaté plus haut que le polynôme $X^4 + X^2 + 1$ n'a pas de racine réelle et pourtant n'est pas irréductible sur $\mathbb{R}$.*

Maintenant, on améliore le théorème 70.

Théorème 72. Soit P un élément de $\mathbb{R}[X]$ de degré supérieur ou égal à 1. Soit $z \in \mathbb{C}$.

z est racine de P si et seulement si $\overline{z}$ est racine de P et dans ce cas, z et $\overline{z}$ ont même ordre de multiplicité.

Démonstration . En ce qui concerne l'ordre de multiplicité d'une racine, on dispose d'une définition et d'une caractérisation à partir des dérivées. Ceci fournit deux démonstrations, présentant chacune leur propre intérêt.

1ère démonstration. Soit P un élément de $\mathbb{R}[X]$ (de sorte que $\overline{P} = P$) de degré supérieur ou égal à 1. Soit $z \in \mathbb{C}$ une racine de P d'ordre $k \in \mathbb{N}^*$. Il existe un polynôme $Q \in \mathbb{C}[X]$ tel que $P = (X-z)^k Q$ et $Q(z) \neq 0$. En conjuguant cette égalité, on obtient $P = (X-\overline{z})^k \overline{Q}$.
De plus, $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$. Donc, $\overline{z}$ est racine de P d'ordre k.

2ème démonstration. Soit P un élément de $\mathbb{R}[X]$ de degré supérieur ou égal à 1 (de sorte que $\overline{P} = P$). Soit $z \in \mathbb{C}$ une racine de P d'ordre $k \in \mathbb{N}^*$. Alors, $P(z) = P'(z) = \ldots = P^{(k-1)}(z) = 0$ et $P^{(k)}(z) \neq 0$.
En conjugant ces égalités et en tenant compte des différentes formules du théorème 69, on obtient $P(\overline{z}) = P'(\overline{z}) = \ldots = P^{(k-1)}(\overline{z}) = 0$ et $P^{(k)}(\overline{z}) \neq 0$. On en déduit que $\overline{z}$ est racine de P d'ordre k.

❑

On peut maintenant se diriger vers la factorisation en produit de facteurs irréductibles dans $\mathbb{R}[X]$. Soit P un élément de $\mathbb{R}[X]$ de degré supérieur ou égal à 1. P est scindé sur $\mathbb{C}$. Notons $a_1, \ldots, a_p$, les éventuelles racines réelles deux à deux distinctes de P, $\alpha_1, \ldots, \alpha_p$, leurs ordres de multiplicité respectifs, $z_1, \ldots, z_q$, les éventuelles racines non réelles de parties imaginaires strictement positives deux à deux distinctes , $\beta_1, \ldots, \beta_q$, leurs ordres de multiplicité respectifs et λ le coefficient dominant de P.

D'après les théorèmes 68 et 72 et avec la convention usuelle qu'un produit vide est nul, P s'écrit, de manière unique à l'ordre près des facteurs, sous la forme :

$$P = \lambda \prod_{k=1}^{p} (X-a_k)^{\alpha_k} \prod_{k=1}^{q} (X-z_k)^{\beta_k} \prod_{k=1}^{q} (X-\overline{z_k})^{\beta_k}.$$

(Si $p = 0$, $\prod_{k=1}^{p} (X-a_k)^{\alpha_k} = 1$ ou si $q = 0$, $\prod_{k=1}^{q} (X-z_k)^{\beta_k} = \prod_{k=1}^{q} (X-\overline{z_k})^{\beta_k} = 1$.) En regroupant les facteurs conjugués, on obtient

$$P = \lambda \prod_{k=1}^{p} (X-a_k)^{\alpha_k} \prod_{k=1}^{q} (X-z_k)^{\beta_k} (X-\overline{z_k})^{\beta_k} = \lambda \prod_{k=1}^{p} (X-a_k)^{\alpha_k} \prod_{k=1}^{q} \left(X^2 + b_k X + c_k\right)^{\beta_k},$$

où $b_k = -2\mathrm{Re}(z_k) \in \mathbb{R}$ et $c_k = |z_k|^2 \in \mathbb{R}$. Cette écriture est encore une fois unique à l'ordre près des facteurs. On note de plus que pour $k \in [\![1, q]\!]$, on a $b_k^2 - 4c_k < 0$ car le trinôme $X^2 + b_k X + c_k$ n'a pas de racine réelle. On peut énoncer

Théorème 73. Tout polynôme de $\mathbb{R}[X]$, de degré supérieur ou égal à 1, s'écrit de manière unique à l'ordre près des facteurs, sous la forme :

$$P = \lambda \prod_{k=1}^{p} (X - a_k)^{\alpha_k} \prod_{k=1}^{q} \left(X^2 + b_k X + c_k\right)^{\beta_k},$$

où $\lambda = \mathrm{dom}(P) \in \mathbb{R}^*$, les a_k sont des réels deux à deux distincts, les (b_k, c_k) sont des couples de réels deux à deux distincts tels que $b_k^2 - 4c_k < 0$, les α_k et les β_k sont des entiers naturels non nuls.

4.5 Quelques factorisations classiques

• Dans $\mathbb{C}[X]$, le polynôme $X^n - 1$ est unitaire et admet n racines simples, les nombres $z_k = e^{\frac{2ik\pi}{n}}$, $0 \leqslant k \leqslant n-1$. Donc,

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

• Dans $\mathbb{R}[X]$, il y a deux cas. Si $n = 2p$, $p \in \mathbb{N}^*$, $X^n - 1 = X^{2p} - 1$ admet deux racines réelles à savoir 1 et -1. En regroupant les facteurs conjugués, on obtient :

$$\begin{aligned} X^{2p} - 1 &= \prod_{k=0}^{2p-1} \left(X - e^{\frac{2ik\pi}{2p}}\right) = (X-1) \times \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{p}}\right) \times (X+1) \times \prod_{k=p+1}^{2p-1} \left(X - e^{\frac{ik\pi}{p}}\right) \\ &= (X-1)(X+1) \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{p}}\right) \prod_{l=1}^{p-1} \left(X - e^{\frac{i(2p-l)\pi}{p}}\right) = (X-1)(X+1) \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{p}}\right)\left(X - e^{-\frac{ik\pi}{p}}\right) \\ &= (X-1)(X+1) \prod_{k=1}^{p-1} \left(X^2 - 2X\cos\left(\frac{k\pi}{p}\right) + 1\right). \end{aligned}$$

Si $n = 2p+1$, $p \in \mathbb{N}^*$, $X^n - 1 = X^{2p+1} - 1$ admet une seule racine réelle à savoir 1. En regroupant les facteurs conjugués, on obtient :

$$\begin{aligned} X^{2p+1} - 1 &= \sum_{k=0}^{2p} \left(X - e^{\frac{2ik\pi}{2p+1}}\right) = (X-1) \times \prod_{k=1}^{p} \left(X - e^{\frac{2ik\pi}{2p+1}}\right) \times \prod_{k=p+1}^{2p} \left(X - e^{\frac{2ik\pi}{2p+1}}\right) \\ &= (X-1) \prod_{k=1}^{p} \left(X - e^{\frac{2ik\pi}{2p+1}}\right)\left(X - e^{-\frac{2ik\pi}{2p+1}}\right) \\ &= (X-1) \prod_{k=1}^{p} \left(X^2 - 2X\cos\left(\frac{2k\pi}{2p+1}\right) + 1\right). \end{aligned}$$

• Dans $\mathbb{C}[X]$, $X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right) = (X-1) \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$ mais aussi $X^n - 1 = (X-1)\left(X^{n-1} + \ldots + X + 1\right)$. Après simplification par le polynôme non nul $X - 1$, on obtient

$$X^{n-1} + \ldots + X + 1 = \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

Ces formules fournissent en particulier :

• $X^2 - 1 = (X-1)(X+1)$.

• Dans $\mathbb{C}[X]$, $X^3 - 1 = (X-1)(X-j)\left(X - j^2\right)$ et aussi $X^2 + X + 1 = (X-j)\left(X - j^2\right)$.
Dans $\mathbb{R}[X]$, $X^3 - 1 = (X-1)\left(X^2 + X + 1\right)$.

• Dans $\mathbb{C}[X]$, $X^4 - 1 = (X-1)(X-i)(X+1)(X+i)$ et aussi $X^3 + X^2 + X + 1 = (X-i)(X+1)(X+i)$.
Dans $\mathbb{R}[X]$, directement $X^4 - 1 = \left(X^2 - 1\right)\left(X^2 + 1\right) = (X-1)(X+1)\left(X^2 + 1\right)$ et $X^3 + X^2 + X + 1 = (X+1)\left(X^2 + 1\right)$.

• Dans $\mathbb{C}[X]$, $X^5-1=(X-1)\left(X-e^{\frac{2i\pi}{5}}\right)\left(X-e^{\frac{4i\pi}{5}}\right)\left(X-e^{-\frac{4i\pi}{5}}\right)\left(X-e^{-\frac{2i\pi}{5}}\right)$.
Dans $\mathbb{R}[X]$, $X^5-1=(X-1)\left(X^2-2X\cos\left(\frac{2\pi}{5}\right)+1\right)\left(X^2-2X\cos\left(\frac{4\pi}{5}\right)+1\right)$.
Dans $\mathbb{C}[X]$, $X^4+X^3+X^2+X+1=\left(X-e^{\frac{2i\pi}{5}}\right)\left(X-e^{\frac{4i\pi}{5}}\right)\left(X-e^{-\frac{4i\pi}{5}}\right)\left(X-e^{-\frac{2i\pi}{5}}\right)$
Dans $\mathbb{R}[X]$, $X^4+X^3+X^2+X+1=\left(X^2-2X\cos\left(\frac{2\pi}{5}\right)+1\right)\left(X^2-2X\cos\left(\frac{4\pi}{5}\right)+1\right)$.

Il se trouve que l'on peut factoriser le polynôme $X^4+X^3+X^2+X+1$ directement en profitant de la symétrie de ses coefficients (polynôme réciproque) :

$$\begin{aligned}X^4+X^3+X^2+X+1&=X^2\left(X^2+\frac{1}{X^2}+X+\frac{1}{X}+1\right)=X^2\left(\left(X+\frac{1}{X}\right)^2+\left(X+\frac{1}{X}\right)-1\right)\\&=X^2\left(X+\frac{1}{X}-\frac{-1+\sqrt{5}}{2}\right)\left(X+\frac{1}{X}-\frac{-1-\sqrt{5}}{2}\right)\\&=\left(X^2-\frac{-1+\sqrt{5}}{2}X+1\right)\left(X^2-\frac{-1-\sqrt{5}}{2}X+1\right).\end{aligned}$$

Par unicité de la décomposition en produit de facteurs irréductibles et en tenant compte de $\cos\left(\frac{2\pi}{5}\right)>0$ et $\cos\left(\frac{4\pi}{5}\right)<0$, on obtient

$$\cos\left(\frac{2\pi}{5}\right)=\frac{-1+\sqrt{5}}{4}\quad\text{et}\quad\cos\left(\frac{4\pi}{5}\right)=\frac{-1-\sqrt{5}}{4}.$$

• Dans $\mathbb{C}[X]$, $X^6-1=(X-1)\left(X+j^2\right)(X-j)(X+1)\left(X-j^2\right)(X+j)$.
Dans $\mathbb{R}[X]$, $X^6-1=(X-1)(X+1)\left(X^2+X+1\right)\left(X^2-X+1\right)$.

• Pour X^4+X^2+1, on peut passer par X^6-1 : $\left(X^2-1\right)\left(X^4+X^2+1\right)=X^6-1=(X-1)(X+1)\left(X^2+X+1\right)\left(X^2-X+1\right)$ et après simplification par le polynôme non nul X^2-1, on obtient :

$$X^4+X^2+1=\left(X^2+X+1\right)\left(X^2-X+1\right).$$

On peut aussi factoriser directement :

$$X^4+X^2+1=X^4+2X^2+1-X^2=\left(X^2+1\right)^2-X^2=\left(X^2+X+1\right)\left(X^2-X+1\right).$$

• Pour X^4-X^2+1, on peut passer par le polynôme X^6+1. Le polynôme X^6+1 est réel et pair. Donc chaque fois que l'on trouve une racine a de ce polynôme, $\overline{a}$ et $-a$ sont aussi racines de ce polynôme. Cette constatation aide à mener les calculs qui suivent :

$$\begin{aligned}X^6+1&=\prod_{k=0}^{5}\left(X-e^{\frac{i(\pi+2k\pi)}{6}}\right)\\&=(X+i)(X-i)\left(X-e^{\frac{i\pi}{6}}\right)\left(X-e^{-\frac{i\pi}{6}}\right)\left(X+e^{\frac{i\pi}{6}}\right)\left(X+e^{-\frac{i\pi}{6}}\right)\\&=\left(X^2+1\right)\left(X^2-2X\cos\left(\frac{\pi}{6}\right)+1\right)\left(X^2+2X\cos\left(\frac{\pi}{6}\right)+1\right)\\&=\left(X^2+1\right)\left(X^2+X\sqrt{3}+1\right)\left(X^2-X\sqrt{3}+1\right).\end{aligned}$$

Mais on a aussi $X^6+1=\left(X^2+1\right)\left(X^4-X^2+1\right)$. Après simplification par le polynôme non nul X^2+1, on obtient :

$$X^4-X^2+1=\left(X^2+X\sqrt{3}+1\right)\left(X^2-X\sqrt{3}+1\right).$$

On peut aussi factoriser directement :

$$X^4-X^2+1=X^4+2X^2+1-3X^2=\left(X^2+1\right)^2-3X^2=\left(X^2+X\sqrt{3}+1\right)\left(X^2-X\sqrt{3}+1\right).$$

Exercice 10.

1) Soit $\theta \in \mathbb{R}$. Soit $A = X^2 - 2X\cos\theta + 1$. Factoriser P en produit de facteurs irréductibles dans $\mathbb{C}[X]$. A quelle condition nécessaire et suffisante P est-il irréductible sur $\mathbb{R}$?

2) Soit $\alpha \in [0, \pi]$. Décomposer en produit de facteurs irréductibles dans $\mathbb{R}[X]$ le polynôme $P = X^6 - 2X^3\cos(3\alpha) + 1$.

Solution 10.

1) Soit $\theta \in \mathbb{R}$. A est irréductible sur $\mathbb{R}$ si et seulement si $\Delta' < 0$ avec $\Delta' = \cos^2\theta - 1 = -\sin^2\theta$. Donc,

$$A \text{ irréductible sur } \mathbb{R} \Leftrightarrow -\sin^2\theta < 0 \Leftrightarrow \sin\theta \neq 0 \Leftrightarrow \theta \notin \pi\mathbb{Z}.$$

Ensuite,

$$X^2 - 2X\cos\theta + 1 = (X - \cos\theta)^2 + \sin^2\theta = (X - \cos\theta - i\sin\theta)(X - \cos\theta + i\sin\theta) = \left(X - e^{i\theta}\right)\left(X - e^{-i\theta}\right).$$

De plus, $e^{i\theta} = e^{-i\theta} \Leftrightarrow e^{2i\theta} = 1 \Leftrightarrow 2\theta \in 2\pi\mathbb{Z} \Leftrightarrow \theta \in \pi\mathbb{Z}$.

Si $\theta \notin \pi\mathbb{Z}$, la décomposition de A en produit de facteurs irréductibles sur $\mathbb{R}$ est : $A = \left(X - e^{i\theta}\right)\left(X - e^{-i\theta}\right)$.
Si $\theta \in 2\pi\mathbb{Z}$, $A = X^2 - 2X + 1 = (X-1)^2$. Si $\theta \in \pi + 2\pi\mathbb{Z}$, $A = X^2 + 2X + 1 = (X+1)^2$.

2) On commence par décomposer P dans $\mathbb{C}[X]$ puis on regroupe les facteurs conjugués. D'après 1),

$$\begin{aligned}
P &= \left(X^3\right)^2 - 2X^3\cos(3\alpha) + 1 = \left(X^3 - e^{3i\alpha}\right)\left(X^3 - e^{-3i\alpha}\right)\\
&= \left(X - e^{i\alpha}\right)\left(X - e^{i\left(\alpha+\frac{2\pi}{3}\right)}\right)\left(X - e^{i\left(\alpha+\frac{4\pi}{3}\right)}\right)\left(X - e^{-i\alpha}\right)\left(X - e^{i\left(-\alpha+\frac{2\pi}{3}\right)}\right)\left(X - e^{i\left(-\alpha+\frac{4\pi}{3}\right)}\right)\\
&= \left(X - e^{i\alpha}\right)\left(X - e^{-i\alpha}\right)\left(X - e^{i\left(\alpha+\frac{2\pi}{3}\right)}\right)\left(X - e^{-i\left(\alpha+\frac{2\pi}{3}\right)}\right)\left(X - e^{i\left(\alpha+\frac{4\pi}{3}\right)}\right)\left(X - e^{-i\left(\alpha+\frac{4\pi}{3}\right)}\right)\\
&= \left(X^2 - 2X\cos\alpha + 1\right)\left(X^2 - 2X\cos\left(\alpha + \frac{2\pi}{3}\right) + 1\right)\left(X^2 - 2X\cos\left(\alpha + \frac{4\pi}{3}\right) + 1\right).
\end{aligned}$$

Il faut ensuite se demander si chacun des trois trinômes est irréductible sur $\mathbb{R}$ et si ces trinômes sont deux à deux distincts. Dans 1), les trois trinômes sont irréductibles sur $\mathbb{R}$ si et seulement si $\alpha \notin \pi\mathbb{Z}$ et $\alpha + \frac{2\pi}{3} \notin \pi\mathbb{Z}$ et $\alpha + \frac{4\pi}{3} \notin \pi\mathbb{Z}$. Puisque $\alpha \in [0, \pi]$, ceci équivaut à $\alpha \notin \left\{0, \frac{\pi}{3}, \frac{2\pi}{3}, \pi\right\}$. Dans ce cas, les trois trinômes sont irréductibles sur $\mathbb{R}$.

D'autre part, pour $\alpha \in [0, \pi]$,

• $\cos\alpha = \cos\left(\alpha + \frac{2\pi}{3}\right) \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha = \alpha + \frac{2\pi}{3} + 2k\pi$ ou $\exists k \in \mathbb{Z}/\ \alpha = -\alpha - \frac{2\pi}{3} + 2k\pi \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha = -\frac{\pi}{3} + k\pi \Leftrightarrow \alpha = \frac{2\pi}{3}$.

• $\cos\alpha = \cos\left(\alpha + \frac{4\pi}{3}\right) \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha = -\alpha - \frac{4\pi}{3} + 2k\pi \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha = -\frac{2\pi}{3} + k\pi \Leftrightarrow \alpha = \frac{\pi}{3}$.

• $\cos\left(\alpha + \frac{2\pi}{3}\right) = \cos\left(\alpha + \frac{4\pi}{3}\right) \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha + \frac{2\pi}{3} = -\alpha - \frac{4\pi}{3} + 2k\pi \Leftrightarrow \exists k \in \mathbb{Z}/\ \alpha = \pi + k\pi \Leftrightarrow \alpha \in \{0, \pi\}$.

1er cas Si $\alpha \in [0, \pi] \setminus \left\{0, \frac{\pi}{3}, \frac{2\pi}{3}, \pi\right\}$, les trois trinômes sont irréductibles sur $\mathbb{R}$ et deux à deux distincts. Dans ce cas, la décomposition de P en produit de facteurs irréductibles sur $\mathbb{R}$ est :

$$P = \left(X^2 - 2X\cos\alpha + 1\right)\left(X^2 - 2X\cos\left(\alpha + \frac{2\pi}{3}\right) + 1\right)\left(X^2 - 2X\cos\left(\alpha + \frac{4\pi}{3}\right) + 1\right).$$

2ème cas. Si $\alpha = 0$ ou $\alpha = \frac{2\pi}{3}$, $P = X^6 - 2X^3 + 1 = \left(X^3 - 1\right)^3 = (X-1)^2\left(X^2 + X + 1\right)^2$.

3ème cas. Si $\alpha = \frac{\pi}{3}$ ou $\alpha = \pi$, $P = X^6 + 2X^3 + 1 = \left(X^3 + 1\right)^2 = (X+1)^2\left(X^2 - X + 1\right)^2$.

4.6 Quelques applications

On analyse dans ce paragraphe comment utiliser la connaissance des racines d'un polynôme (ou ce qui revient au même, de sa factorisation) en arithmétique des polynômes. On commence par le très important résultat :

Théorème 74. Soient A et B deux éléments non nuls de $\mathbb{K}[X]$, $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, de degrés supérieurs ou égaux à 1.

A et B sont premiers entre eux (dans $\mathbb{K}[X]$) si et seulement si A et B n'ont pas de racine commune dans $\mathbb{C}$.

Démonstration .

• Si A et B ne sont pas premiers entre eux, on peut écrire $A=DA_1$, $B=DB_1$, avec $(D,A_1,B_1)\in(\mathbb{K}[X]\setminus\{0\})^3$, $\deg(D)\geqslant 1$, $A_1\wedge B_1=1$.
Puisque $\deg(D)\geqslant 1$, D a au moins une racine dans $\mathbb{C}$. Cette racine est alors une racine commune à A et à B.

• Si A et B sont premiers entre eux, il existe $(U,V)\in\mathbb{K}[X]^2$ tel que $AU+BV=1$. En particulier, $\forall z\in\mathbb{C}$, $A(z)U(z)+B(z)V(z)\neq 0$. A et B ne peuvent donc avoir de racine commune.

❑

Théorème 75. Soit A un élément de $\mathbb{C}[X]$ de degré supérieur ou égal à 1.

A est à racines simples $\Leftrightarrow$ A et A' n'ont pas de racine commune $\Leftrightarrow$ $A\wedge A'=1$.

Démonstration .

Si A et A' ont une racine en commun, alors cette racine est racine d'ordre au moins 2 de A.
Si A et A' n'ont pas de racine commune, alors en particulier, une racine de A n'est pas racine de A' et est donc une racine simple de A.
En résumé, A est à racines simples (dans $\mathbb{C}$) si et seulement si A et A' n'ont pas de racine commune.

D'après le théorème précédent, cette dernière condition est équivalente à $A\wedge A'=1$.

❑

Considérons le polynôme $P=X^n-1$, $n\geqslant 2$. On sait que ce polynôme a n racines deux à deux distinctes (et donc simples) à savoir les n racines n-èmes de l'unité dans $\mathbb{C}$: $z_k=e^{\frac{2ik\pi}{n}}$, $k\in[\![0,n-1]\!]$.
Mais si nous n'avions pas résolu l'équation $z^n=1$ plus tôt dans l'année et donc, si nous ne connaissions pas les racines du polynôme X^n-1, on serait quand même capable de voir rapidement que ses racines sont simples.
En effet, une racine multiple a de X^n-1 dans $\mathbb{C}$ est une racine de $P=X^n-1$ et de $P'=nX^{n-1}$. En tant que racine de P', on a nécessairement $a=0$ mais 0 n'est pas racine de P. Donc, P et P' n'ont pas de racine commune dans $\mathbb{C}$ et donc les racines de P sont simples.
On aurait aussi pu constater que $(-1)P+\left(\frac{1}{n}X\right)P'=(-1)\left(X^n-1\right)+\left(\frac{1}{n}X\right)\left(nX^{n-1}\right)=1$ et donc P et P' sont premiers entre eux d'après le théorème de Bézout. De nouveau, P est à racines simples dans $\mathbb{C}$.

Exercice 11. Pour $n\geqslant 2$, on pose $P_n=\sum_{k=0}^{n}\frac{X^k}{k!}$.

Montrer que les racines de P_n dans $\mathbb{C}$ sont simples.

Solution 11. $P_n=\frac{X^n}{n!}+\frac{X^{n-1}}{(n-1)!}+\ldots+\frac{X^1}{1!}+1$ et $P_n'=\frac{X^{n-1}}{(n-1)!}+\ldots+\frac{X^1}{1!}+1$. Une éventuelle racine commune a à P_n et P_n' dans $\mathbb{C}$ est encore racine de $P_n-P_n'=\frac{X^n}{n!}$ et est donc nulle. Mais 0 n'est pas racine de P_n.

Donc, P_n et P_n' n'ont pas de racines communes dans $\mathbb{C}$ puis P_n est à racines simples dans $\mathbb{C}$.

Enfin, la factorisation en produit de facteurs irréductibles dans $\mathbb{C}[X]$ permet de déterminer facilement le PPCM et le PGCD de deux polynômes :

Théorème 76. Soient A et B deux éléments non nuls de $\mathbb{C}[X]$, de degrés supérieurs ou égaux à 1 et unitaires. Si on pose

$$A=\prod_{k=1}^{p}(X-a_k)^{\alpha_k} \quad \text{et} \quad B=\prod_{k=1}^{p}(X-a_k)^{\beta_k}$$

où les a_k sont des nombres complexes deux à deux distincts et les α_k sont des entiers naturels, alors

$$A\wedge B=\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}} \quad \text{et} \quad A\vee B=\prod_{k=1}^{p}(X-a_k)^{\text{Max}\{\alpha_k,\beta_k\}}$$

Démonstration. Pour tout $k\in[\![1,p]\!]$, $\alpha_k-\text{Min}\{\alpha_k,\beta_k\}\geqslant 0$ avec égalité si et seulement si $\alpha_k\leqslant\beta_k$. De même, $\beta_k-\text{Min}\{\alpha_k,\beta_k\}\geqslant 0$ avec égalité si et seulement si $\beta_k\leqslant\alpha_k$.

On peut donc écrire $A=DA_1$ et $B=DB_1$ avec $D=\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}}\in\mathbb{C}[X]$, $A_1=\prod_{k=1}^{p}(X-a_k)^{\alpha_k-\text{Min}\{\alpha_k,\beta_k\}}\in\mathbb{C}[X]$ et $B_1=\prod_{k=1}^{p}(X-a_k)^{\beta_k-\text{Min}\{\alpha_k,\beta_k\}}\in\mathbb{C}[X]$.

Si pour un certain $k\in[\![1,p]\!]$, $\alpha_k-\text{Min}\{\alpha_k,\beta_k\}\neq 0$, alors $\alpha_k>\beta_k$ puis $\beta_k-\text{Min}\{\alpha_k,\beta_k\}=0$ et de même, si $\beta_k-\text{Min}\{\alpha_k,\beta_k\}\neq 0$, alors $\alpha_k-\text{Min}\{\alpha_k,\beta_k\}=0$. Ainsi, les polynômes A_1 et B_1 n'ont pas de racines communes dans $\mathbb{C}$ et sont donc premiers entre eux. Mais alors

$$A\wedge B=(DA_1)\wedge(DB_1)=D(A_1\wedge B_1)=D=\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}}.$$

Ensuite, pour tout $k\in[\![1,p]\!]$, $\alpha_k+\beta_k=\text{Min}\{\alpha_k,\beta_k\}+\text{Min}\{\alpha_k,\beta_k\}$. Donc,

$$\begin{aligned}(A\vee B)\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}}&=(A\vee B)(A\wedge B)=AB\\&=\prod_{k=1}^{p}(X-a_k)^{\alpha_k+\beta_k}=\prod_{k=1}^{p}(X-a_k)^{\text{Max}\{\alpha_k,\beta_k\}}\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}}.\end{aligned}$$

Après simplification par le polynôme non nul $\prod_{k=1}^{p}(X-a_k)^{\text{Min}\{\alpha_k,\beta_k\}}$, on obtient

$$A\vee B=\prod_{k=1}^{p}(X-a_k)^{\text{Max}\{\alpha_k,\beta_k\}}.$$

❑

Ainsi, si $A=(X-1)^2(X-2)(X-3)^3=(X-1)^2(X-2)^1(X-3)^3(X-4)^0$ et $B=(X-1)(X-3)^5(X-4)=(X-1)^1(X-2)^0(X-3)^5(X-4)^1$, $A\wedge B=(X-1)(X-3)^3$ et $A\vee B=(X-1)^2(X-2)(X-3)^5(X-4)$.

5 Relations entre coefficients et racines d'un polynôme de $\mathbb{C}[X]$

Commençons par rappeler le cas du degré 2. Soit $P=aX^2+bX+c$, $(a,b,c)\in(\mathbb{C}\setminus\{0\})\times\mathbb{C}\times\mathbb{C}$. P admet dans $\mathbb{C}$ deux racines z_1 et z_2, distinctes ou confondues et on peut écrire

$$P=aX^2+bX+c=a(X-z_1)(X-z_2)=a\left(X^2-(z_1+z_2)X+z_1z_2\right).$$

En identifiant les coefficients, on obtient les relations entre coefficients et racines d'un trinôme du second degré :

$$z_1+z_2=-\frac{b}{a} \quad \text{et} \quad z_1z_2=\frac{c}{a}.$$

Passons au degré 3. Soit $P=aX^3+bX^2+cX+d$, $(a,b,c,d)\in(\mathbb{C}\setminus\{0\})\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}$. P admet dans $\mathbb{C}$ trois racines z_1, z_2 et z_3 et on peut écrire

$$\begin{aligned}P&=aX^3+bX+c=a(X-z_1)(X-z_2)(X-z_3)\\&=a\left(X^3-(z_1+z_2+z_3)X^2+(z_1z_2+z_1z_3+z_2z_3)X-z_1z_2z_3\right).\end{aligned}$$

En identifiant les coefficients, on obtient les relations entre coefficients et racines d'un polynôme du troisième degré :

$$z_1+z_2+z_3=-\frac{b}{a} \quad \text{et} \quad z_1z_2+z_1z_3+z_2z_3=\frac{c}{a} \quad \text{et} \quad z_1z_2z_3=-\frac{d}{a}.$$

Les trois expressions $z_1+z_2+z_3$, $z_1z_2+z_1z_3+z_2z_3$ et $z_1z_2z_3$ sont les trois **fonctions symétriques élémentaires** en z_1, z_2 et z_3, symétriques car la valeur de chacune de ces expressions est invariante par toute permutation des variables z_1, z_2 et z_3. On les note respectivement σ_1, σ_2 et σ_3 :

$$\sigma_1=z_1+z_2+z_3 \quad \text{et} \quad \sigma_2=z_1z_2+z_1z_3+z_2z_3 \quad \text{et} \quad \sigma_3=z_1z_2z_3.$$

Par exemple, si z_1, z_2 et z_3 sont les trois racines du polynôme X^3+2X^2+1, on a $z_1+z_2+z_3=\sigma_1=-\frac{2}{1}=-2$, $z_1z_2+z_1z_3+z_2z_3=\sigma_2=0$ et $z_1z_2z_3=\sigma_3=-\frac{1}{1}=-1$. On note que l'on sait fournir ces égalités sans pour autant savoir calculer z_1, z_2 et z_3.

Passons maintenant au cas général. Soit $n\geqslant 2$. Soit $P=\sum_{k=0}^{n}a_kX^k$ où $a_0,\ldots,a_n$, sont n nombres complexes, a_n étant non nul. Soient $z_1,\ldots,z_n$, les n racines de P dans $\mathbb{C}$ (les z_k n'étant pas nécessairement deux à deux distincts). On a

$$a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0=a_n\left(X-z_1\right)\times\ldots\times\left(X-z_n\right).$$

Il nous reste à savoir développer le produit ci-dessus pour pouvoir ensuite identifier les coefficients. C'est un produit de n facteurs, chaque facteur étant composé de deux termes. Après développement et avant réduction, on obtient une somme de $2\times2\times\ldots\times2=2^n$ termes du type $X\left(-z_2\right)\left(-z_3\right)XXX\left(-z_7\right)\ldots$
On regroupe les termes comportant un même nombre k ($0\leqslant k\leqslant n$) de lettres X ou encore, on cherche le coefficient de X^k. Ces termes sont du type $\left(-z_{i_1}\right)\ldots\left(-z_{i_{n-k}}\right)X^k=(-1)^{n-k}z_{i_1}\ldots z_{i_{n-k}}X^k$ où $i_1,\ldots,i_{n-k}$ sont des indices deux à deux distincts. Le coefficient de X^k est alors la somme de ces $(-1)^{n-k}z_{i_1}\ldots z_{i_{n-k}}$ où, pour être sûr de ne pas répéter plusieurs fois un même terme (par exemple $z_2z_3z_1=z_1z_2z_3$), les numéros $i_1,\ldots,i_{n-k}$ sont classés dans l'ordre croissant : $i_1<i_2<\ldots<i_{n-k}$.

On est donc amené à définir les n **fonctions symétriques élémentaires** en $z_1,\ldots,z_n$:

Pour $k\in[\![1,n]\!]$, on pose $\sigma_k=\sum_{\substack{(i_1,\ldots,i_k)\in[\![1,n]\!]^k\\ i_1<i_2<\ldots<i_k}}z_{i_1}\ldots z_{i_k}$.

σ_k est la somme des produits k à k des nombres $z_1,\ldots,z_n$. En particulier, σ_1 est la somme des nombres $z_1,\ldots,z_n$ et σ_n est le produit des nombres $z_1,\ldots,z_n$:

$$\boxed{\sigma_1=z_1+z_2+\ldots+z_n \quad \text{et} \quad \sigma_n=z_1\ldots z_n.}$$

Le développement de $a_n\left(X-z_1\right)\ldots\left(X-z_n\right)$ est alors

$$\begin{aligned}a_n\left(X-z_1\right)\ldots\left(X-z_n\right)&=a_n\left(X^n-\sigma_1X^{n-2}+\sigma_2X^{n-2}+\ldots+(-1)^{n-k}\sigma_{n-k}X^k+\ldots+(-1)^{n-1}\sigma_{n-1}X+(-1)^n\sigma_n\right)\\&=a_n\sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}X^k,\end{aligned}$$

avec la convention $\sigma_0=1$. En identifiant les coefficients, on obtient pour tout $k\in[\![0,n]\!]$, $a_k=a_n(-1)^{n-k}\sigma_{n-k}$, égalités qui se réécrivent sous la forme $\sigma_k=(-1)^k\frac{a_{n-k}}{a_n}$. On a obtenu les **relations entre coefficients et racines** d'un polynôme :

Théorème 77. Soient $n\geqslant2$ puis $P=\sum_{k=0}^{n}a_kX^k$ où $a_0,\ldots,a_n$, sont n nombres complexes, a_n étant non nul. Soient $z_1,\ldots,z_n$, les n racines de P dans $\mathbb{C}$.

Pour $k\in[\![1,n]\!]$, on pose $\sigma_k=\sum_{\substack{(i_1,\ldots,i_k)\in[\![1,n]\!]^k\\ i_1<i_2<\ldots<i_k}}z_{i_1}\ldots z_{i_k}$. Alors,

$$\forall k\in[\![1,n]\!],\ \sigma_k=(-1)^k\frac{a_{n-k}}{a_n}.$$

En particulier,

$$z_1+\ldots+z_n=-\frac{a_{n-1}}{a_n} \quad \text{et} \quad z_1\ldots z_n=(-1)^n\frac{a_0}{a_n}.$$

Exercice 12. Soient z_1, z_2 et z_3 les trois racines dans $\mathbb{C}$ du polynôme $P = X^3 + X + 1$.

Calculer $\dfrac{1}{z_1} + \dfrac{1}{z_2} + \dfrac{1}{z_3}$ et $z_1^2 + z_2^2 + z_3^2$.

Solution 12. On a $z_1 + z_2 + z_3 = \sigma_1 = -\dfrac{0}{1} = 0$, $z_1z_2 + z_1z_3 + z_2z_3 = \sigma_2 = +\dfrac{1}{1} = 1$ et $z_1z_2z_3 = -\dfrac{1}{1} = -1$. En particulier, $z_1z_2z_3 \neq 0$ et donc aucun des z_i n'est égal à 0.

- $\dfrac{1}{z_1} + \dfrac{1}{z_2} + \dfrac{1}{z_3} = \dfrac{z_1z_2 + z_1z_3 + z_2z_3}{z_1z_2z_3} = \dfrac{\sigma_2}{\sigma_3} = -1$.
- $z_1^2 + z_2^2 + z_3^2 = (z_1 + z_2 + z_3)^2 - 2(z_1z_2 + z_1z_3 + z_2z_3) = \sigma_1^2 - 2\sigma_2 = -2$.

---

6 Familles célèbres de polynômes

Dans ce paragraphe, on se contente de citer quelques familles célèbres de polynômes qui constituent des thèmes classiques de problèmes de concours. Il y a énormément à dire sur chacune de ces familles de polynômes qui, suivant le cas, ont été utilisées en algèbre, en analyse, en probabilité, en physique théorique ... On détaille uniquement (en partie) le cas des polynômes de Tchebychev.

6.1 Polynômes de Lagrange

On a déjà étudié la famille des polynômes de Lagrange (voir page 34). On se contente d'en rappeler une expression.

Soient $a_0, \dots, a_n$, $n+1$ nombres complexes deux à deux distincts. Pour $i \in [\![0, n]\!]$, on pose

$$L_i = \prod_{\substack{j \in [\![0,n]\!] \\ j \neq i}} \frac{X - a_j}{a_i - a_j}.$$

Chaque polynôme L_i est de degré n. La famille de polynômes $(L_i)_{0 \leqslant i \leqslant n}$ vérifient les égalités :

$$\forall (i,j) \in [\![0,n]\!]^2,\ L_i(a_j) = \delta_{i,j}.$$

Si $b_0, \dots, b_n$, sont $n+1$ nombres complexes donnés, les L_i servent à exprimer l'unique polynôme L de degré inférieur ou égal à n vérifiant les égalités : $\forall i \in [\![0,n]\!]$, $L(a_i) = b_i$:

$$L = \sum_{i=0}^{n} b_i L_i.$$

6.2 Polynômes de Tchebychev

• **Existence et unicité (et définition) de T_n et U_n.** Montrons que pour tout naturel n, il existe un et un seul polynôme T_n tel que

$$\boxed{\forall \theta \in \mathbb{R},\ \cos(n\theta) = T_n(\cos\theta),}$$

et que, pour tout naturel non nul n, il existe un et un seul polynôme U_n tel que

$$\boxed{\forall \theta \in \mathbb{R},\ \sin(n\theta) = \sin\theta\, U_n(\cos\theta).}$$

Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$. D'après la formule du binôme de Newton, on a :

$$\begin{aligned}
\cos(n\theta) + i\sin(n\theta) = e^{in\theta} = \left(e^{i\theta}\right)^n = (\cos\theta + i\sin\theta)^n &= \sum_{k=0}^{n} \binom{n}{k} (\cos\theta)^{n-k} (i\sin\theta)^k \\
&= \sum_{k=0}^{E(n/2)} \binom{n}{2k} (\cos\theta)^{n-2k} (i\sin\theta)^{2k} + \sum_{k=0}^{E((n-1)/2)} \binom{n}{2k+1} (\cos\theta)^{n-(2k+1)} (i\sin\theta)^{2k+1} \\
&= \sum_{k=0}^{E(n/2)} (-1)^k \binom{n}{2k} (\cos\theta)^{n-2k} (1-\cos^2\theta)^k + i\sin\theta \sum_{k=0}^{E((n-1)/2)} (-1)^k \binom{n}{2k+1} (\cos\theta)^{n-(2k+1)} (1-\cos^2\theta)^k
\end{aligned}$$

Par identification des parties réelles et imaginaires, on obtient :

$$\cos(n\theta) = \sum_{k=0}^{E(n/2)} (-1)^k \binom{n}{2k} (\cos\theta)^{n-2k} (1-\cos^2\theta)^k,$$

et

$$\sin(n\theta) = \sin\theta \sum_{k=0}^{E((n-1)/2)} (-1)^k \binom{n}{2k+1} (\cos\theta)^{n-(2k+1)} (1-\cos^2\theta)^k.$$

Posons alors

$$\boxed{T_n = \sum_{k=0}^{E(n/2)} (-1)^k \binom{n}{2k} X^{n-2k}(1-X^2)^k \text{ et } U_n = \sum_{k=0}^{E((n-1)/2)} (-1)^k \binom{n}{2k+1} X^{n-(2k+1)}(1-X^2)^k.}$$

Ces polynômes conviennent. Ceci montre l'existence de T_n et U_n.

Soient P et Q deux polynômes. Si, pour tout réel θ, $P(\cos\theta) = \cos(n\theta) = Q(\cos\theta)$, alors, pour tout réel x de $[-1,1]$, $P(x) = Q(x)$. Mais alors, les polynômes P et Q coïncident en une infinité de valeurs de la variable x et sont donc égaux. On en déduit l'unicité de T_n.

De même, si, pour tout réel θ, $\sin\theta P(\cos\theta) = \sin(n\theta) = \sin\theta Q(\cos\theta)$, alors, pour tout réel θ non dans $\pi\mathbb{Z}$, $P(\cos\theta) = Q(\cos\theta)$, puis pour tout réel x de $]-1,1[$, $P(x) = Q(x)$. De nouveau, les polynômes P et Q coïncident en une infinité de valeurs de la variable x et sont donc égaux. On en déduit l'unicité de U_n.

T_n et U_n s'appellent respectivement les n-èmes polynômes de Tchebychev de première espèce et de deuxième espèce.

• Montrons que

$$\boxed{\forall n \in \mathbb{N}^*,\ T_n' = nU_n.}$$

Soit $n \in \mathbb{N}^*$. En dérivant l'égalité définissant T_n, on obtient pour tout réel θ :

$$-\sin\theta T_n'(\cos\theta) = -n\sin(n\theta) = -n\sin\theta U_n(\cos\theta),$$

et donc, pour tout réel θ non dans $\pi\mathbb{Z}$,

$$T_n'(\cos\theta) = nU_n(\cos\theta).$$

Par suite, pour tout réel x de $]-1,1[$, on a $T_n'(x) = nU_n(x)$. Ainsi, les polynômes T_n' et nU_n coïncident en une infinité de valeurs et sont donc égaux.

• Donnons les premières valeurs des polynômes T_n et U_n. On a $T_1 = X$, $T_2 = 2X^2 - 1$, $T_3 = 4X^3 - 3X$ (car pour tout réel θ, $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$) puis

$$T_4 = \sum_{k=0}^{2} (-1)^k \binom{4}{2k} X^{4-2k}\left(1-X^2\right)^k = X^4 - 6X^2\left(1-X^2\right) + \left(1-X^2\right)^2 = 8X^4 - 8X^2 + 1.$$

Ensuite, $U_1 = T_1' = 1$, $U_2 = \frac{1}{2}T_2' = 2X$, $U_3 = \frac{1}{3}T_3' = 4X^2 - 1$, $U_4 = \frac{1}{4}T_4' = 8X^3 - 4X$.

$T_1 = X$	$U_1 = 1$
$T_2 = 2X^2 - 1$	$U_2 = 2X$
$T_3 = 4X^3 - 3X$	$U_3 = 4X^2 - 1$
$T_4 = 8X^4 - 8X^2 + 1$	$U_4 = 8X^3 - 4X$

On étudie dorénavant les polynômes de Tchebychev de première espèce.

• Degré et coefficient dominant de T_n.

On a déjà $\deg T_0 = 0$ et $\mathrm{dom} T_0 = 1$. Soit alors n un entier naturel non nul. On rappelle que

$$T_n = \sum_{k=0}^{E(n/2)} (-1)^k \binom{n}{2k} X^{n-2k}\left(1-X^2\right)^k.$$

Pour $k \in \left\{0, ..., E\left(\frac{n}{2}\right)\right\}$, le polynôme $X^{n-2k}(1-X^2)^k$ est de degré $n-2k+2k=n$. Donc, T_n est de degré au plus n. De plus, le coefficient de X^n dans T_n vaut

$$\sum_{k=0}^{E(n/2)}(-1)^k\binom{n}{2k}(-1)^k = \sum_{k=0}^{E(n/2)}\binom{n}{2k} = \frac{1}{2}\left(\left(\binom{n}{0}+\binom{n}{1}+...+\binom{n}{n}\right)+\left(\binom{n}{0}-\binom{n}{1}+...+(-1)^n\binom{n}{n}\right)\right)$$
$$= \frac{1}{2}\left((1+1)^n+(1-1)^n\right) = 2^{n-1} \ (0^n = 0 \text{ car } n \geqslant 1).$$

Donc,

$$\boxed{\deg T_0 = 0 \text{ et } \mathrm{dom} T_0 = 1 \text{ puis } \forall n \in \mathbb{N}^*, \ \deg T_n = n \text{ et } \mathrm{dom} T_n = 2^{n-1}.}$$

• Quelques valeurs prises par T_n. Soit $n \in \mathbb{N}$. $T_n(1) = T_n(\cos 0) = \cos(n \times 0) = 1$. Ensuite, $T_n(-1) = T_n(\cos\pi) = \cos(n\pi) = (-1)^n$. Enfin, $T_n(0) = T_n\left(\cos\frac{\pi}{2}\right) = \cos\left(n\frac{\pi}{2}\right) = \begin{cases} 0 \text{ si } n \text{ est impair.} \\ (-1)^{n/2} \text{ si } n \text{ est pair.} \end{cases}$.

$$\boxed{\forall n \in \mathbb{N}, \ T_n(1) = 1, \ T_n(-1) = (-1)^n, \ T_n(0) = \begin{cases} 0 \text{ si } n \text{ est impair.} \\ (-1)^{n/2} \text{ si } n \text{ est pair.} \end{cases}.}$$

• Parité de T_n. Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$.

$$T_n(-\cos\theta) = T_n(\cos(\theta+\pi)) = \cos(n\theta+n\pi) = (-1)^n\cos(n\theta) = (-1)^n T_n(\cos\theta).$$

Par suite,

$$\forall n \in \mathbb{N}, \ \forall x \in [-1,1], \ T_n(-x) = (-1)^n T_n(x).$$

Les deux polynômes $T_n(-X)$ et $(-1)^n T_n$ coïncident donc en une infinité de valeurs de x et sont par suite égaux.

$$\boxed{\forall n \in \mathbb{N}, \ T_n(-X) = (-1)^n T_n.}$$

T_n a donc la parité de n.

• Relation de récurrence. Pour tout réel θ, on a $\cos(n\theta)+\cos((n+2)\theta) = 2\cos\theta\cos((n+1)\theta)$, ce qui s'écrit encore

$$\forall n \in \mathbb{N}, \ \forall \theta \in \mathbb{R}, \ T_{n+2}(\cos\theta) - 2\cos\theta T_{n+1}(\cos\theta) + T_n(\cos\theta) = 0$$

ou encore

$$\forall n \in \mathbb{N}, \ \forall x \in [-1,1], \ T_{n+2}(x) - 2xT_{n+1}(x) + T_n(x) = 0,$$

ou enfin, puisque le polynôme $T_{n+2} - 2XT_{n+1} + T_n$ a une infinité de racines,

$$\boxed{\forall n \in \mathbb{N}, \ T_{n+2} - 2XT_{n+1} + T_n = 0}.$$

• Equation différentielle vérifiée par T_n. Soit $n \in \mathbb{N}$. Pour tout réel θ, on a

$$-n^2 T_n(\cos\theta) = -n^2\cos(n\theta) = (\cos(n\theta))'' = (T_n(\cos\theta))'' = (-\sin\theta T_n'(\cos\theta))'$$
$$= -\cos\theta T_n'(\cos\theta) + \sin^2\theta T_n''(\cos\theta) = -\cos\theta T_n'(\cos\theta) + (1-\cos^2\theta)T_n''(\cos\theta).$$

Par suite,

$$\forall x \in [-1,1], \ n^2 T_n(x) - xT_n'(x) + (1-x^2)T_n''(x) = 0,$$

et finalement (polynôme ayant une infinité de racines)

$$\boxed{\forall n \in \mathbb{N}, \ n^2 T_n - XT_n' + (1-X^2)T_n'' = 0}.$$

• Coefficients de T_n. Soit $n \in \mathbb{N}^*$. Puisque T_n a la parité de n, on peut poser $T_n = a_0X^n + a_1X^{n-2} + ... = \sum_{k=0}^{E(n/2)} a_kX^{n-2k}$.

Avec ces notations, on a

$$\begin{aligned}
&n^2T_n - XT_n' + (1-X^2)T_n'' \\
&= n^2 \sum_{k=0}^{E(n/2)} a_kX^{n-2k} - X \sum_{k=0}^{E((n-1)/2)} (n-2k)a_kX^{n-2k-1} + (1-X^2) \sum_{k=0}^{E(n/2)-1} (n-2k)(n-2k-1)a_kX^{n-2k-2} \\
&= \sum_{k=0}^{E(n/2)} n^2a_kX^{n-2k} - \sum_{k=0}^{E(n/2)} (n-2k)a_kX^{n-2k} + \sum_{k=0}^{E(n/2)-1} (n-2k)(n-2k-1)a_kX^{n-2k-2} \\
&\quad - \sum_{k=0}^{E(n/2)} (n-2k)(n-2k-1)a_kX^{n-2k} \\
&= \sum_{k=0}^{E(n/2)} (n^2 - (n-2k) - (n-2k)(n-2k-1))a_kX^{n-2k} + \sum_{k=0}^{E(n/2)-1} (n-2k)(n-2k-1)a_kX^{n-2k-2} \\
&= \sum_{k=0}^{E(n/2)} (n^2 - (n-2k) - (n-2k)(n-2k-1))a_kX^{n-2k} + \sum_{k=1}^{E(n/2)} (n-2k+2)(n-2k+1)a_{k-1}X^{n-2k} \\
&= \sum_{k=1}^{E(n/2)} (4k(n-k)a_k + (n-2k+2)(n-2k+1)a_{k-1})X^{n-2k}.
\end{aligned}$$

En tenant compte de $a_0 = \mathrm{dom}(T_n) = 2^{n-1}$ (pour $n \geqslant 1$) et puisque le polynôme précédent est nul, on obtient :

$$a_0 = 2^{n-1} \text{ et } \forall k \in \{1, ..., E(n/2)\},\ a_k = -\frac{(n-2k+1)(n-2k+2)}{4k(n-k)}a_{k-1}.$$

Mais alors, pour $k \in \{1, ..., E(n/2)\}$,

$$\begin{aligned}
a_k &= (-1)^k \frac{(n-2k+1)(n-2k+2)(n-2k+3)(n-2k+4)...(n-1)n}{4^k k(k-1)...1(n-k)(n-k+1)...(n-1)}a_0 = (-1)^k 2^{n-1-2k} \frac{n!(n-k-1)!}{(n-2k)!k!(n-1)!} \\
&= (-1)^k 2^{n-1-2k} \frac{n}{n-k} \frac{(n-k)!}{(n-2k)!k!} = (-1)^k 2^{n-1-2k} \frac{n}{n-k} \binom{n-k}{k},
\end{aligned}$$

ce qui reste vrai pour $k = 0$. Donc,

$$\forall k \in \left\{0, ..., E\left(\frac{n}{2}\right)\right\},\ a_k = (-1)^k 2^{n-1-2k} \frac{n}{n-k} \binom{n-k}{k},$$

ou encore,

$$\boxed{\forall n \in \mathbb{N}^*,\ T_n = \sum_{k=0}^{E(n/2)} (-1)^k 2^{n-2k-1} \frac{n}{n-k} \binom{n-k}{k} X^{n-2k}.}$$

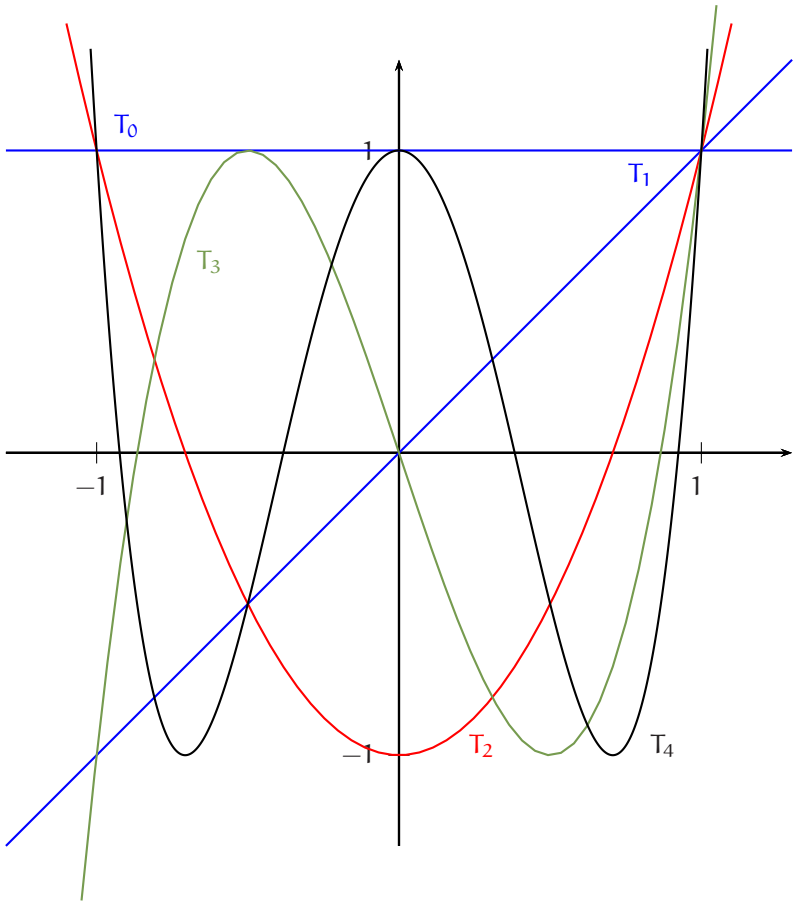
• Racines de T_n et factorisation. Soit $n \in \mathbb{N}^*$. Pour tout réel θ,

$$T_n(\cos\theta) = 0 \Leftrightarrow \cos(n\theta) = 0 \Leftrightarrow n\theta \in \frac{\pi}{2} + \pi\mathbb{Z} \Leftrightarrow \theta \in \frac{\pi}{2n} + \frac{\pi}{n}\mathbb{Z}.$$

Pour $k \in [\![0, n-1]\!]$, posons $\theta_k = \frac{\pi}{2n} + \frac{k\pi}{n}$ puis $x_k = \cos\theta_k$. Les n nombres θ_k sont deux à deux distincts et dans $[0, \pi]$ (car $0 \leqslant \frac{\pi}{2n} \leqslant \frac{\pi}{2n} + \frac{k\pi}{n} \leqslant \frac{\pi}{2n} + \frac{(n-1)\pi}{n} = \pi - \frac{\pi}{2n} \leqslant \pi$). Par injectivité de cos sur $[0, \pi]$, les n nombres x_k sont deux à deux distincts et tous racines du polynôme T_n qui est de degré n. On a ainsi trouvé toutes les racines de T_n, toutes simples, réelles et dans $[-1, 1]$. On en déduit la factorisation suivante de T_n (en tant compte de $\mathrm{dom}(T_n) = 2^{n-1}$) :

$$\boxed{\forall n \in \mathbb{N}^*,\ T_n = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)\right).}$$

• Quelques graphes.



6.3 Polynômes de Legendre

Une définition possible des polynômes de Legendre L_n est :

$$\forall n \in \mathbb{N},\ L_n = \left(\left(X^2-1\right)^n\right)^{(n)}.$$

Dans ce chapitre, on a vérifié en exercice que $\deg(L_n)$, $\mathrm{dom}(L_n) = \dfrac{(2n)!}{n!}$ et que L_n a n racines réelles simples, toutes dans $]-1,1[$.

6.4 Polynômes d'Hermite

Une définition possible des polynômes de Hermite H_n est :

$$\forall n \in \mathbb{N},\ H_n = (-1)^n e^{X^2}\left(e^{-X^2}\right)^{(n)}.$$

Malgré la présence de l'exponentielle, H_n est effectivement un polynôme.
Par exemple, $H_2 = e^{X^2}\left(-2Xe^{-X^2}\right)' = e^{X^2}\left(-2e^{-X^2}+4X^2e^{-X^2}\right) = 4X^2-2$.

6.5 Polynômes de Bernoulli

Les polynômes de Bernoulli B_n sont définis par récurrence par :

$$B_0 = 1,\ \forall n \in \mathbb{N},\ B'_{n+1} = (n+1)B_n \text{ et } \forall n \in \mathbb{N}^*,\ \int_0^1 B_n(t)\,dt = 0.$$

Ces polynômes servent « entre autres » à calculer les sommes $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$, ... ou aussi les sommes infinies $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$, $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n^4} = \frac{\pi^4}{90}$, ...

6.6 Polynômes de Bernstein

Si f est une fonction définie sur $[0,1]$ à valeurs dans $\mathbb{R}$ (ou $\mathbb{C}$), le n-ème polynôme de Bernstein associé à f est :

$$B_n(f) = \sum_{k=0}^{n} \binom{n}{k} f\left(\frac{k}{n}\right) X^k (1-X)^{n-k}.$$

On peut montrer que, si f est continue sur $[0,1]$, pour n grand, le graphe de $B_n(f)$ sur $[0,1]$ est très proche du graphe de f.