POLYNÔMES

▶ Arithmétique sur les polynômes

1. *Enoncé : Soit $n \geq 2$. Effectuer la division euclidienne de A par B dans $\mathbb{K}[X]$, lorsque :*
   (a) $A = X^3 + X^2 - X + 1, B = X - 1$;
   On a :
$$\begin{array}{rrrr|l}
X^3 & +X^2 & -X & +1 & X-1 \\ \cline{5-5}
-X^3 & +X^2 & & & X^2+2X+1 \\ \cline{1-2}
 & 2X^2 & -X & & \\
 & -2X^2 & +2X & & \\ \cline{2-3}
 & & X & +1 & \\
 & & -X & +1 & \\ \cline{3-4}
 & & & 2 &
\end{array}$$
   (b) $A = X^4 - 3X^3 + 4X^2 - 1, B = X^2 + X + 1$;
   On a :
$$\begin{array}{rrrrr|l}
X^4 & -3X^3 & +4X^2 & & -1 & X^2+X+1 \\ \cline{6-6}
-X^4 & -X^3 & -X^2 & & & X^2-4X+7 \\ \cline{1-3}
 & -4X^3 & +3X^2 & & & \\
 & 4X^3 & +4X^2 & +4X & & \\ \cline{2-4}
 & & 7X^2 & +4X & -1 & \\
 & & -7X^2 & -7X & -7 & \\ \cline{3-5}
 & & & -3X & -8 &
\end{array}$$
   (c) $A = X^5 + X^4 - X^3 + X - 1, B = X^3 + X^2 + 2$;
   On a :
$$\begin{array}{rrrrrr|l}
X^5 & +X^4 & -X^3 & & +X & -1 & X^3+X^2+2 \\ \cline{7-7}
-X^5 & -X^4 & & -2X^2 & & & X^2-1 \\ \cline{1-4}
 & & -X^3 & -2X^2 & +X & -1 & \\
 & & X^3 & +X^2 & & +2 & \\ \cline{3-6}
 & & & -X^2 & +X & +1 &
\end{array}$$
   (d) $A = X^{3n+2} + X^{3n+1} + X^{3n}, B = X^2 + X + 1$;
   On a :
$$\begin{aligned} A &= X^{3n+2} + X^{3n+1} + X^{3n} \\ &= (X^{3n})(X^2 + X + 1) \end{aligned}$$
   Donc par unicité de la division euclidienne, on a :
$$A = (X^{3n})B$$
   (e) $A = X^{n+2} + X^{n+1} - X^n, B = X^3 - 2X + 1$;
   On a :
$$\begin{array}{r|r}
x^{n+2} + x^{n+1} - x^n & x^3 - 2x + 1 \\ \cline{2-2}
-x^{n+2} + 2x^n - x^{n-1} & x^{n-1} + x^{n-2} + x^{n-3} \\ \cline{1-1}
x^{n+1} + x^n - x^{n-1} & \\
-x^{n+1} + 2x^{n-1} - x^{n-2} & \\ \cline{1-1}
x^n + x^{n-1} - x^{n-2} &
\end{array}$$

Donc on remarque que :

$$A = (X^3 - 2X + 1)\sum_{k=0}^{n-1} X^k + R$$

Donc :

$$\begin{aligned} R &= X^{n+2} + X^{n+1} - X^n - (X^3 - 2X + 1)\frac{X^n - 1}{X - 1} \\ &= X^{n+2} + X^{n+1} - X^n - (X - 1)(X^2 + X - 1)\frac{X^n - 1}{X - 1} \\ &= X^{n+2} + X^{n+1} - X^n - (X^2 + X - 1)(X^n - 1) \\ &= X^{n+2} + X^{n+1} - X^n - (X^{n+2} + X^{n+1} - X^n - X^2 - X + 1) \\ &= X^2 + X - 1 \end{aligned}$$

Donc :

$$A = (X^3 - 2X + 1)\sum_{k=0}^{n-1} X^k + (X^2 + X - 1)$$

<u>Autre méthode :</u>

On a :

$$\begin{aligned} &A = BQ + R \\ &R = aX^2 + bX + C \quad \text{car } \deg(R) < \deg(B) = 2 \end{aligned}$$

Trouvons les racines de B :

1 est racine de B, donc on a $B = (X - 1)(X^2 + X - 1)$.

Les racines du polynomes $X^2 + X - 1$ sont :

$$\psi = \frac{-1 + \sqrt{5}}{2} \quad \text{et} \quad \bar{\psi} = \frac{-1 - \sqrt{5}}{2}$$

Donc on a :

$$\begin{cases} R(1) &= A(1) \\ R(\psi) &= A(\psi) \\ R(\bar{\psi}) &= A(\bar{\psi}) \end{cases} \iff \begin{cases} a + b + c = 1 \\ a\psi^2 + b\psi + c = \psi^{n+2} + \psi^{n+1} - \psi^n = \psi^n(\psi^2 + \psi - 1) = 0 \\ a\bar{\psi}^2 + b\bar{\psi} + c = \bar{\psi}^{n+2} + \bar{\psi}^{n+1} - \bar{\psi}^n = \bar{\psi}^n(\bar{\psi}^2 + \bar{\psi} - 1) = 0 \end{cases}$$

R est une polynome de degré ≤ 2 unique.

Or $x^2 + x - 1$ vérifie le système avec $a = 1$, $b = 1$, $c = -1$

Ou sinon, R est un polynôme de degré 2 tel que : $R(\psi) = R(\bar{\psi}) = 0$ et donc on a :

$$(X - \psi)(X - \bar{\psi}) \mid R$$

Donc :

$$X^2 + X - 1 \mid aX^2 + bX + c$$

Par degrée, $\exists \lambda \in \mathbb{K}$ tel que :

$$aX^2 + bX + c = \lambda(X^2 + X - 1)$$

Donc $\lambda = 1$ et $R = X^2 + X - 1$.

(f) $A = (X-3)^{2n} + (X-2)^n - 2, B = (X-2)^2$;
On a :
$$\exists! Q \in \mathbb{K}[X], \exists!(a,b) \in \mathbb{K}^2 \quad \text{tels que} \quad A = BQ + aX + b$$
De plus, en $x = 2$, on a :
$$A(2) = (-1)^{2n} - 2 = -1 = 2a + b$$
En dérivant :
$$A' = B'Q + Q'B + q$$
En $x = 2$, on a :
$$A'(2) = a = -2n$$
Donc : $\begin{cases} a = -2n \\ b = -1 - 2a = 4n - 1 \end{cases}$ Et donc : $R = -2nX + 4n - 1$.

(g) $A = X^n, B = X - 1$.
On a :
$$(X-1)\sum_{k=0}^{n-1} X^k = X^n - 1^n = X^n - 1$$
$$X^n - 1 + 1 = X^n$$
Donc par unicité de la division euclidienne, on a :
$$A = (X-1)\sum_{k=0}^{n-1} X^k + 1$$

2. *Enoncé : Soit* $P = X^6 - 2X^5 - 8X^4 - 22X^3 - 53X^2 - 56X - 20$.

(a) Calculer le reste de la division euclidienne de P par $X^2 + 1$.
On a :
$$\begin{array}{l|l}
X^6 - 2X^5 - 8X^4 - 22X^3 - 53X^2 - 56X - 20 & X^2 + 1 \\ \cline{2-2}
\underline{-X^6 \qquad\quad - X^4} & X^4 - 2X^3 - 9X^2 - 20X - 44 \\
\quad -2X^5 - 9X^4 - 22X^3 & \\
\quad \underline{2X^5 \qquad\quad + 2X^3} & \\
\qquad -9X^4 - 20X^3 - 53X^2 & \\
\qquad \underline{9X^4 \qquad\quad + 9X^2} & \\
\qquad\quad -20X^3 - 44X^2 - 56X & \\
\qquad\quad \underline{20X^3 \qquad\quad + 20X} & \\
\qquad\qquad -44X^2 - 36X - 20 & \\
\qquad\qquad \underline{44X^2 \qquad\quad + 44} & \\
\qquad\qquad\qquad -36X + 24 &
\end{array}$$

(b) Calculer $P(\mathrm{i})$.
Avec a) on sait que :
$$P = (X^2+1)(X^4 - 2X^3 - 9X^2 - 20X - 44) + (-36X + 24)$$
Donc :
$$P(\mathrm{i}) = (-36\mathrm{i} + 24)$$

3. *Enoncé : Soit $P \in \mathbb{K}[X]$.*
   (a) *Démontrer que $P - X$ divise $P^k - X^k$ pour tout $k \geq 1$.*
   Posons $P = \sum_{k=0}^{\infty} a_k X^k$.
   Alors :
   $$P^k - X^k = (P - X) \sum_{j=0}^{k-1} P^j X^{k-j}$$
   Donc $P - X$ divise $P^k - X^k$ pour tout $k \geq 1$.
   (b) *En déduire que $P - X$ divise $P \circ P - P$.*
   On a :
   $$\begin{aligned} P \circ P - P &= P(P(X)) - P(X) \\ &= \sum_{k=0}^{\infty} a_k P(X)^k - \sum_{k=0}^{\infty} a_k X^k \\ &= \sum_{k=0}^{\infty} a_k \underbrace{\left(P(X)^k - X^k\right)}_{\text{divisible par } P-X} \end{aligned}$$
   Donc par a), on a :
   $$P - X \mid P \circ P - P$$
   (c) *Conclure en démontrant que $P - X$ divise $P \circ P - X$.*
   On a :
   $$P \circ P - X = (P \circ P - P) + (P - X)$$
   Donc par b), on a :
   $$P - X \mid P \circ P - X$$
4. *Enoncé : Déterminer le pgcd des polynômes $X^5 + X^3 + X^2 + 1$ et $2X^3 + 1$.*

$$\begin{array}{r|l} X^5 + X^3 + X^2 + 1 & 2X^3 + 1 \\ \cline{2-2} -X^5 \quad - \frac{1}{2}X^2 & \frac{1}{2}X^2 + \frac{1}{2} \\ \hline X^3 + \frac{1}{2}X^2 + 1 & \\ -X^3 \quad - \frac{1}{2} & \\ \hline \frac{1}{2}X^2 + \frac{1}{2} & \end{array} \qquad \begin{array}{r|l} 2X^3 \quad + 1 & \frac{1}{2}X^2 + \frac{1}{2} \\ \cline{2-2} -2X^3 - 2X & 4X \\ \hline -2X + 1 & \end{array} \qquad \begin{array}{r|l} \frac{1}{2}X^2 \quad + \frac{1}{2} & -2X + 1 \\ \cline{2-2} -\frac{1}{2}X^2 + \frac{1}{4}X & -\frac{1}{4}X - \frac{1}{8} \\ \hline \frac{1}{4}X + \frac{1}{2} & \\ -\frac{1}{4}X + \frac{1}{8} & \\ \hline \frac{5}{8} & \end{array}$$

$$\begin{array}{r|l} -2X + 1 & \frac{5}{8} \\ \cline{2-2} 2X \quad & -\frac{16}{5}X + \frac{8}{5} \\ \hline 1 & \\ -1 & \\ \hline 0 & \end{array}$$

$$\begin{aligned} X^5 + X^3 + X^2 + 1 &= (2X^3 + 1)\left(\frac{1}{2}X^2 + \frac{1}{2}\right) + \left(\frac{1}{2}X^2 + \frac{1}{2}\right) \\ 2X^3 + 1 &= \left(\frac{1}{2}X^2 + \frac{1}{2}\right)(4X) + (-2X + 1) \\ \frac{1}{2}X^2 + \frac{1}{2} &= (-2X + 1)\left(-\frac{1}{4}X - \frac{1}{8}\right) + \frac{5}{8} \\ -2X + 1 &= \frac{5}{8}\left(-\frac{16}{5}X + \frac{8}{4}\right) + 0 \end{aligned}$$

Donc le pgcd est 1.

5. *Enoncé :*

   (a) *Soient $a, b \in \mathbb{C}$ tels que $a \neq b$ et soit $P \in \mathbb{C}[X]$. Déterminer le reste de la division euclidienne de P par $(X-a)(X-b)$.*
   Soit $P \in \mathbb{C}[X]$.
   Posons $R : X \mapsto \alpha X + \beta$ avec $\alpha, \beta \in \mathbb{C}$ un polynôme de degrée 2.
   On a :

   $$P(X) = (X-a)(X-b)Q(X) + R(X)$$

   Trouvons les racines pour remonter à α et β.
   On a :
   $$\begin{cases} P(a) = R(a) = \alpha a + \beta \\ P(b) = R(b) = \alpha b + \beta \end{cases} \iff \begin{cases} \frac{P(a)-P(a)}{(a-b)} = \alpha \\ P(a) - \frac{P(b)-P(a)}{(b-a)} = \beta \end{cases}$$
   Donc on a :

   $$R(X) = \frac{P(a)-P(b)}{a-b}X + P(a) - \frac{P(b)-P(a)}{b-a} \quad \text{avec } a \neq b$$

   (b) *Soit $\varphi \in \mathbb{R}$. Déterminer le reste de la division euclidienne de $(\cos\varphi + X\sin\varphi)^n$ par X^2+1.*
   Soit $\varphi \in \mathbb{R}$.
   On divise $(\cos\varphi + X\sin\varphi)^n$ par un polynome de degré 2.
   On pose :
   $$R_2 : X \mapsto \alpha X + \beta \quad \text{avec } \alpha, \beta \in \mathbb{R}$$
   Les racines de X^2+1 sont i et $-$i.
   On a :

   $$(\cos\varphi + i\sin\varphi)^n = \alpha i + \beta \iff e^{in\varphi} = \alpha i + \beta$$
   $$(\cos\varphi - i\sin\varphi)^n = \alpha(-i) + \beta \iff e^{-in\varphi} = -\alpha i + \beta$$

   Donc on a le système :

   $$\begin{cases} \alpha i + \beta = e^{in\varphi} \\ -\alpha i + \beta = e^{-in\varphi} \end{cases} \iff \begin{cases} \alpha = \frac{e^{in\varphi}-e^{-in\varphi}}{2i} = \sin(n\varphi) \\ \beta = \frac{e^{in\varphi}+e^{-in\varphi}}{2} = \cos(n\varphi) \end{cases}$$

   Donc :
   $$R(X) = \sin(n\varphi)X + \cos(n\varphi)$$

▶ Racines

6. *Enoncé : Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $\forall z \in \mathbb{C}, P(z) = \bar{z}$.*
   Analyse :
   Supposons trouvé $P \in \mathbb{C}[X]$ tel que :

   $$\forall z \in \mathbb{C}, \quad P(z) = \bar{z}$$

Posons $Q(X) = P(X) - X$.
Donc :
$$\forall x \in \mathbb{R}, \quad Q(X) = P(X) - X = \bar{X} - X = 0$$
Donc Q admet une infinité de racines réelles, donc Q est le polynôme nul.
Alors :
$$\forall z \in \mathbb{C}, \quad Q(z) = P(z) - z = 0$$
Donc $P(z) = z$ pour tout $z \in \mathbb{C}$.
Ce qui veut dire que $\bar{z} = z$ pour tout $z \in \mathbb{C}$.
Absurde. Donc il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que $\forall z \in \mathbb{C}, P(z) = \bar{z}$.

7. *Enoncé : Soit I un intervalle de $\mathbb{R}$ non vide, non réduit à un point et f, g deux fonctions polynomiales telles que $\forall x \in I, f(x)g(x) = 0$. Démontrer que $f = 0$ ou $g = 0$. Ce résultat s'applique-t-il aux fonctions non polynomiales ?*
Il existe $a, b \in I$ tels que $a < b$.
Donc par convexité de I, on a $[a, b] \subset I$.
Donc I contient une infinité de points compris entre a et b.
Donc le polynome $f \times g$ admet une infinité de racines dans I.
Donc le polynôme $f \times g$ est le polynôme nul.
Par intégrité de l'anneau $\mathbb{K}[X]$, on a :
$$f = 0 \quad \text{ou} \quad g = 0$$
Contre-exemple :
Soit $f : X \mapsto \mathbb{1}_{\{0\}}$ et $g : X \mapsto \mathbb{1}_{\{1\}}$.
On a bien $\forall x \in I, f(x)g(x) = 0$ mais $f \neq 0$ et $g \neq 0$.

8. *Enoncé : Résoudre dans $\mathbb{C}$ les systèmes suivants :*
$$\text{(a)} \begin{cases} x + y = 3 \\ x^2 + y^2 = 5 \end{cases} ; \text{(b)} \begin{cases} x + y + z & = 1 \\ x^2 + y^2 + z^2 & = 9 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} & = 1 \end{cases} .$$
(a) :
Soit $x, y \in \mathbb{C}$, on a :
$$\begin{cases} x + y = 3 \\ x^2 + y^2 = 5 \end{cases} \iff \begin{cases} x^2 + 2xy + y^2 = 9 \\ x^2 + y^2 = 5 \end{cases} \iff \begin{cases} xy = 2 \\ x^2 + y^2 = 5 \end{cases}$$
On peut alors construire le polynôme caractéristique associé au systeme :
$$P(X) = X^2 - (x + y)X + xy = X^2 - 3X + 2 = (X - 1)(X - 2)$$
Donc les solutions sont $x = 1$ et $y = 2$ ou $x = 2$ et $y = 1$.
(b) :
Soit $x, y, z \in \mathbb{C}$, on a :

$$\begin{cases} x+y+z=1 \\ x^2+y^2+z^2=9 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \end{cases} \iff \begin{cases} x^2+y^2+z^2+2(xy+xz+yz)=1 \\ x^2+y^2+z^2=9 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \end{cases}$$

$$\iff \begin{cases} xy+xz+yz=-4 \\ x+y+z=1 \\ \frac{xy+xz+yz}{xyz}=1 \end{cases}$$

$$\iff \begin{cases} xy+xz+yz=-4 \\ x+y+z=1 \\ xyz=-4 \end{cases}$$

On peut alors construire le polynôme caractéristique associé au systeme :

$$\begin{aligned} P(X) &= X^3-(x+y+z)X^2+(xy+xz+yz)X-xyz \\ &= X^3-X^2-4X+4 \\ &= (X-1)(X^2-4) \\ &= (X-1)(X-2)(X+2) \end{aligned}$$

Donc les solutions sont : $(x,y,z) \in \{(1,2,-2),(1,-2,2),(2,1,-2),(2,-2,1),(-2,1,2),(-2,2,1)\}$

9. *Enoncé : Soit $P \in \mathbb{K}[X]$ tel que $P(0)=0$ et $P\left(X^2+1\right)=P^2+1$.*

   (a) *On considère la suite définie par récurrence par $u_0=0$ et $u_{n+1}=u_n^2+1$ pour $n \geq 0$. Démontrer que, pour tout $n \in \mathbb{N}, P\left(u_n\right)=u_n$.*

   Montrons par récurrence sur n, que pour tout $n \in \mathbb{N}$, on a :

   $$\mathrm{P}(n) : "P(u_n)=u_n"$$

   Initialisation : Pour $n=0$, on a :

   $$P(u_0)=P(0)=0=u_0$$

   Hérédité :
   Supposons que pour un $n \in \mathbb{N}$, on a : $P(u_n)=u_n$.
   Montrons que pour $n+1$, on a : $P(u_{n+1})=u_{n+1}$.
   On a :

   $$\begin{aligned} P(u_{n+1}) &= P(u_n^2+1) \\ &= P^2(u_n)+1 \\ &= u_n^2+1 \quad \text{(H.R)} \\ &= u_{n+1} \end{aligned}$$

   Donc $\mathrm{P}(n+1)$ est vrai.
   La propriété est héréditaire.
   Conclusion :
   Donc pour tout $n \in \mathbb{N}$, on a : $P(u_n)=u_n$.

(b) *Que peut-on en déduire sur le polynôme P ?*
Posons le polynome $Q(X) = P(X) - X$.
On a :

$$Q(u_n) = P(u_n) - u_n = 0$$

Or $\forall n \geq 1, u_n \geq 1$ et donc $u_{n+1} > u_n$.
Donc $(u_n)_n$ est strictement croissante, donc Q admet une infinité de racines distinctes dans $\mathbb{R}$.
Donc Q est le polynôme nul et $P(X) = X$.

10. *Enoncé : Soient $n, p \in \mathbb{N}^*$. Démontrer que :*

$$(X^n - 1) \wedge (X^p - 1) = X^{n \wedge p} - 1$$

Soit $n, p \in \mathbb{N}^*$.
Montrons que $(X^n - 1) \wedge (X^p - 1) = X^{n \wedge p} - 1$.
Quitte à échanger n et p, on suppose que $p \leq n$.
Si $n = p$, alors $n \wedge p = n$ et on a :

$$(X^n - 1) \wedge (X^p - 1) = (X^n - 1) \wedge (X^n - 1) = X^n - 1 = X^{n \wedge p} - 1$$

Sinon, par algorithme d'Euclide sur $\mathbb{Z}$:
Il existe $(r_k)_k$ et un entier $N > 0$ tel que $\forall k \geq N, r_{k+2}$ est le reste de la division euclidienne de r_k par r_{k+1} si $r_{k+1} \neq 0$ (sinon $r_{k+2} = 0$).
On a donc :

$$\begin{cases} r_{N+1} = 0 \\ r_N = n \wedge p \\ \forall k \geq N, r_{k+1} = r_{k-1} \wedge r_k = n \wedge p \end{cases}$$

Appliquons l'algorithme d'Euclide sur les $\mathbb{K}[X]$.
Donc $n = pq + r_2$ avec $q \in \mathbb{N}$ et $0 \leq r_2 < p$.
Donc on a :

$$X^n - 1 = X^{pq+r_2} - 1 = (X^p - 1)(?) + (X^{r_2} - 1)$$

Or :

$$\begin{aligned} X^{pq+r_2} - 1 &= (X^{pq})X^{r_2} - 1 \\ &= (X^{pq} - 1 + 1)X^{r_2} - 1 \\ &= (X^{pq} - 1)X^{r_2} + (X^{r_2} - 1) \\ &= (X^p - 1)\sum_{k=0}^{q-1} X^{kp+r_2} + (X^{r_2} - 1) \end{aligned}$$

Donc on a :

$$X^n - 1 = (X^p - 1)\sum_{k=0}^{q-1} X^{kp+r_2} + (X^{r_2} - 1)$$

Donc $X^{r_2} - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^p - 1$.
Donc on a :

$$(X^n - 1) \wedge (X^p - 1) = (X^p - 1) \wedge (X^{r_2} - 1)$$

Egalement, en partant de $r_k = q_k r_{k+1} + r_{k+2}$ avec $q_k \in \mathbb{N}$, le reste de $(X^{r_n} - 1)$ et $(X^{r_{n+1}} - 1)$ est $(X^{r_{n+2}} - 1)$.
Donc on a :

$$\forall k \leq N, \quad (X^n - 1) \wedge (X^p - 1) = (X^{r_n} - 1) \wedge (X^{r_{n+1}} - 1)$$

Et en $k = N$, on a :

$$\begin{cases} r_{N+1} = 0 \\ r_N = n \wedge p \end{cases}$$

Donc :

$$(X^p - 1) \wedge (X^n - 1) = (X^{r_N} - 1) \wedge (X^{N+1} - 1) = (X^{n \wedge p} - 1) \wedge (X^0 - 1) = (X^{n \wedge p} - 1)$$

11. *Enoncé : Soient x, y, z trois complexes non nuls tels que $x + y + z = 0$ et $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 0$. Montrer que $|x| = |y| = |z|$.*
Soit $x, y, z \in \mathbb{C}^*$
On a le systeme :

$$\begin{cases} x + y + z = 0 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 0 \end{cases} \iff \begin{cases} x + y + z = 0 \\ \frac{yz+xz+xy}{xyz} = 0 \end{cases} \iff \begin{cases} xyz \neq 0 \\ x + y + z = 0 \\ yz + xz + xy = 0 \end{cases}$$

Si on pose le polynome associé au système, on obtient :

$$(X - x)(X - y)(X - z) = X^3 - (x + y + z)X^2 + (xy + yz + zx)X - xyz$$

Posons $K = xyz \in \mathbb{C}$ de tel manière à ce que $K \neq 0$ et :

$$P(X) = X^3 - K$$

Posons $K = re^{i\theta}$ avec $r > 0$ et $\theta \in \mathbb{R}$.
Alors les racines de P sont les racines cubiques de K :

$$\sqrt[3]{r} \times e^{i\frac{\theta}{3}} \times e^{\frac{2k\pi}{3}} \quad \text{pour } k = 0, 1, 2$$

Posons $X_1 = \sqrt[3]{r}e^{i\frac{\theta}{3}}$, $X_2 = \sqrt[3]{r}e^{i(\frac{\theta}{3}+\frac{2\pi}{3})}$ et $X_3 = \sqrt[3]{r}e^{i(\frac{\theta}{3}+\frac{4\pi}{3})}$.
Donc les solutions du système sont :

$$(x, y, z) \in \{(X_1, X_2, X_3), (X_1, X_3, X_2), (X_2, X_1, X_3), (X_2, X_3, X_1), (X_3, X_1, X_2), (X_3, X_2, X_1)\}$$

Et dans tout les cas, on a :

$$|x| = |y| = |z| = \sqrt[3]{r}$$

12. *Enoncé : Soit $n \in \mathbb{N}$. Le polynôme*

$$P_n = \sum_{k=0}^{n} \frac{\mathrm{X}^k}{k!}$$

possède-t-il une racine multiple ?

Posons :

$$P_n = \sum_{k=0}^{n} \frac{X^k}{k!} \quad \text{et} \quad P_n' = P_{n-1} = \sum_{k=0}^{n-1} \frac{X^k}{k!}.$$

Alors, si $a \in \mathbb{K}$ est racine multiple de P_n, alors :

$$P_n(a) = P_n'(a) = 0$$

Donc :

$$P_n(a) = P_{n-1}(a) = 0$$

Or $P_n = \frac{X^n}{n!} + P_{n-1}$.
Donc :

$$\begin{aligned} & \frac{a^n}{n!} + P_{n-1}(a) = P_{n-1}(a) = 0 \\ \iff & \frac{a^n}{n!} = 0 \\ \iff & a^n = 0 \\ \iff & a = 0 \end{aligned}$$

Or $P_n(0) = 1 \neq 0$. Donc P_n n'admet pas de racine multiple.

▸ Dérivation

13. *Enoncé : Résoudre dans $\mathbb{C}[X]$ l'équation $P(3X) = P' + 5P''$.*
Analyse :
Soit $P \in \mathbb{C}[X]$ tel que : $P(3X) = P' + 5P''$.
Posons $D = \deg(P)$.
Alors :

$$\begin{aligned} \deg(P(3X)) &= D \times 1 = D \\ \deg(P' + 5P'') \leq \deg(P') &= D - 1 \end{aligned}$$

Donc $D \leq D - 1$, ce qui est absurde.
D'ou $D = -\infty$, donc P est le polynôme nul.
Synthèse :
Si $P = 0$, alors on a bien $P(3X) = 0 = P' + 5P''$.

14. *Enoncé : Déterminer tous les polynômes $P \in \mathbb{K}[X]$ tels que $P(1) = 1, P'(1) = 0, P''(1) = 3$ et $P^{(n)}(1) = 0$ pour $n \geq 3$.*
Soit $P \in \mathbb{K}[X]$ tel que :

$$P(1) = 1, P'(1) = 0, P''(1) = 3 \text{ et } P^{(n)}(1) = 0 \text{ pour } n \geq 3$$

.
D'après la formule de Taylor, on a :

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(1)}{k!}(X-1)^k$$

Donc on a :

$$P = \frac{P^0(1)}{0!}(X-1)^0 + \frac{P^1(1)}{1!}(X-1)^1 + \frac{P^2(1)}{2!}(X-1)^2$$

Avec les conditions initiales, on a :

$$P = 1 + 0 + \frac{3}{2}(X-1)^2 = 1 + \frac{3}{2}X^2 - 3X + \frac{3}{2}$$

Donc on a :

$$P = \frac{3}{2}X^2 - 3X + \frac{5}{2}$$

15. *Enoncé : Démontrer que pour tout $n \in \mathbb{N}^*, (X-1)^3$ divise le polynôme*

$$P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n.$$

Soit $n \in \mathbb{N}^*$.
On a :

$$\begin{aligned} P_n &= nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n \\ P_n' &= n(n+2)X^{n+1} - (n+2)(n+1)X^n + (n+2) \\ P_n'' &= n(n+2)(n+1)X^n - (n+2)(n+1)nX^{n-1} \\ P_n''' &= n^2(n+2)(n+1)X^{n-1} - (n+2)(n+1)n(n-1)X^{n-2} \end{aligned}$$

Et en $X = 1$, on a :

$$\begin{aligned} P_n(1) &= n - (n+2) + (n+2) - n = 0 \\ P_n'(1) &= n(n+2) - (n+2)(n+1) + (n+2) = 0 \\ P_n''(1) &= n(n+2)(n+1) - (n+2)(n+1)n = 0 \end{aligned}$$

Donc 1 est au moins racine triple de P_n.
On a donc :

$$P_n = (X-1)^3 Q(X) \text{ avec } Q(X) \in \mathbb{K}[X].$$

Et $(X-1)^3 \mid P_n$.

16. *Enoncé : Déterminer tous les polynômes $P \in \mathbb{R}[X]$ tels que*

$$\forall k \in \mathbb{Z}, \int_k^{k+1} P(t)\mathrm{d}t = k+1$$

<u>Analyse :</u>
Supposons trouver $P \in \mathbb{R}[X]$ tel que :

$$\forall k \in \mathbb{Z}, \int_k^{k+1} P(t)\mathrm{d}t = k+1$$

Posons $Q(X)$ la primitive de P donnée par :

$$Q : X \mapsto \int_0^X P(t)\mathrm{d}t$$

Alors on a :

$$\begin{aligned}
Q(k+1) - Q(k) &= k+1 \\
\sum_{k=0}^{n-1} (Q(k+1) - Q(k)) &= \sum_{k=0}^{n-1} (k+1) \\
Q(n) - Q(0) &= \sum_{k=0}^{n-1} k + n - 1 \\
Q(n) &= \frac{(n-1)n}{2} + n - 1 + Q(0) \\
&= (n-1)\left(\frac{n}{2} + 1\right) + Q(0)
\end{aligned}$$

Posons $R : X \mapsto (X-1)\left(\frac{X}{2}+1\right) + Q(0)$
Donc $\forall x \in \mathbb{R}$, on a :

$$R(x) = \frac{X^2}{2} + \frac{X}{2} - 1 + Q(0)$$

De plus, $Q(0) = \int_0^0 P(t)\mathrm{d}t = 0$ donc :

$$R(x) = \frac{X^2}{2} + \frac{X}{2} - 1$$

Et :

$$R'(x) = X + \frac{1}{2}$$

R prend toutes les valeurs de Q sur $\mathbb{N}$, donc en posant $D = R - Q$, $\forall n \geq 0, D(n) = 0$.
Donc D admet une infinité de racines et donc $R = Q$.
Donc P est la dérivée de R et donc :

$$P(X) = R'(X) = X + \frac{1}{2}$$

Synthèse :
Considérons le polynôme $P(X) = X + \frac{1}{2}$.

$$\int_k^{k+1} P(t)\mathrm{d}t = \int_k^{k+1} \left(t + \frac{1}{2}\right)\mathrm{d}t = \left[\frac{t^2}{2} + \frac{1}{2}t\right]_k^{k+1} = \left(\frac{(k+1)^2}{2} + \frac{k+1}{2}\right) - \left(\frac{k^2}{2} + \frac{k}{2}\right) = k+1$$

Donc P vérifie bien la condition.

17. *Enoncé : Soit $P \in \mathbb{K}[X]$. Démontrer que*

$$P(X+1) = \sum_{n=0}^{+\infty} \frac{1}{n!} P^{(n)}$$

Soit $P \in \mathbb{K}[X]$, montrons que :

$$P(X+1) = \sum_{k=0}^{+\infty} \frac{1}{k!} P^{(k)}(X)$$

Par taylor, soit $a \in \mathbb{K}$, on a :

$$\begin{aligned}
P(X) &= \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-a)^k \\
P(X+1) &= \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}((X+1)-a)^k \\
&= \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}(X-(a-1))^k \\
P(a+1) &= \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}
\end{aligned}$$

Posons :

$$R = \sum_{k=0}^{+\infty} \frac{P^{(k)}(X)}{k!} - \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!}((X+1)-a)^k$$

Donc, $\forall a \in \mathbb{K}$, on a :

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

Donc en identifiant $\mathbb{K}[X]$ à $\mathbb{K}[x]$, on a :

$$R = 0 \quad \text{et} \quad P(X+1) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(X)}{k!}$$

18. *Enoncé : Déterminer tous les polynômes divisibles par leur polynôme dérivé.*
Soit $P \in \mathbb{K}[X]$ tel que $P \mid P'$.
Sur $\mathbb{C}[X]$, P est scindé, donc on peut écrire :

$$P = c \prod_{k=1}^{n} (X - z_k)^{\mu_k}$$

Avec : $\begin{cases} c \in \mathbb{K} \quad \text{le coefficient dominant du polynôme} \\ z_1, \dots, z_n \in \mathbb{C} \quad \text{les racines de } P \\ \mu_1, \dots, \mu_n \in \mathbb{N}^* \quad \text{les multiplicité des racines de } P \end{cases}$

Analyse :
Supposons que $P' \mid P$.
Donc :

$$\forall x \in \mathbb{K} \text{ tel que } P'(x) = 0, \quad P(x) = 0$$

Donc les racines de P' sont aussi des racines de P.
Sur $\mathbb{C}[X]$, quitte à permuter les racines, on peut supposer que $z_1, \dots, z_m$ avec $m \leq n$ sont les racines de P'.
Donc on peut écrire :

$$P' = \hat{c} \prod_{k=1}^{m} (X - z_k)^{\mu_k - 1}$$

Avec : $\begin{cases} \hat{c} \in \mathbb{K} \quad \text{le coefficient dominant du polynôme} \\ z_1, \ldots, z_m \in \mathbb{C} \quad \text{les racines de } P' \\ \mu_1, \ldots, \mu_m \in \mathbb{N}^* \geq 2 \quad \text{car } (X - z_k)^2 | P \end{cases}$

En passant au degré :

$$\deg(P') = \sum_{k=1}^{m} \mu_k - 1 = \sum_{k=1}^{m} (\mu_k) - n$$

Et en supposant que $\deg(P) \geq 1$, on a :

$$\deg(P') = \deg(P) - 1 \geq 0$$

Donc on a :

$$\begin{aligned} \sum_{k=1}^{m} \mu_k - 1 &= \sum_{k=1}^{n} \mu_k - n \\ \sum_{k=1}^{n} \mu_k - \sum_{k=1}^{m} \mu_k &= -n + 1 \\ \underbrace{\sum_{k=m+1}^{n} \mu_k}_{\geq 0} &= \underbrace{-(n-1)}_{\leq 0} \end{aligned}$$

Car $z_{m+1}, \ldots, z_n$ sont des racines de P mais pas de P'.
Donc $m = 1$
Donc P est de la forme :

$$P = c(X - z_1)^n$$

<u>Synthèse :</u>
On a bien $P' = cn(X - z_1)^{n-1} \mid P$.

19. *Enoncé : Soit $P \in \mathbb{R}[X]$ un polynôme scindé de degré $n \geq 2$. Démontrer que P' est scindé.*
Soit $P \in \mathbb{R}[X]$ un polynôme scindé de degré $n \geq 2$.
Démontrons que P' est scindé.
Posons :

$$P = c \prod_{k=1}^{n} (X - x_k)^{\mu_k} \text{ avec } \begin{cases} c \in \mathbb{R} \quad \text{le coefficient dominant du polynôme} \\ x_1, \ldots, x_n \in \mathbb{R} \quad \text{les racines distinctes de } P \\ \mu_1, \ldots, \mu_n \in \mathbb{N}^* \quad \text{les multiplicité des racines de } P \end{cases}$$

Et $\deg(P) = d = \sum_{k=1}^{n} \mu_k$.
Quitte à permuter les racines, on peut supposer que $x_1 < x_2 < \ldots < x_m < \ldots < x_n$ avec $x_1, \ldots, x_m$ les racines simples de P.
Soit $k \in [\![1, n-1]\!]$.

Alors : $\begin{cases} P(x_k) = 0 \\ P(x_{k+1}) = 0 \\ P \text{ est continue sur } [x_k, x_{k+1}] \\ P \text{ est dérivable sur }]x_k, x_{k+1}[\end{cases}$ Donc par théorème de Rolle :

$$\exists z_k \in [x_k, x_{k+1}] \text{ tel que } P'(z_k) = 0$$

Comme les z_k sont 2 à 2 distinctes, on a $n-1$ racines distinctes de P'.
Donc :

$$\prod_{k=1}^{n-1}(X-z_k) \mid P'$$

Posons :

$$\mathcal{E} = \{k \in [\![1, n]\!] \mid \mu_k \geq 2\}$$

Alors, $\forall k \in \mathcal{E}, (X-x_k)^{\mu_k - 1} \mid P'$.
On pose $Q = \prod_{k=1}^{n-1}(X-z_k) \prod_{k\in\mathcal{E}}(X-x_k)^{\mu_k-1}$.
Donc on a :

$$Q \mid P'$$

Et en passant au degré, on a :

$$\begin{aligned}\deg(Q) &= (n-1) + \sum_{k\in\mathcal{E}}(\mu_k - 1) \\ &= (n-1) + \sum_{k\in\mathcal{E}}(\mu_k) - \operatorname{card}(\mathcal{E})\end{aligned}$$

Or :

$$\begin{aligned}\deg(P) &= \sum_{k=1}^{n}\mu_k \\ &= \sum_{k\in\mathcal{E}}(\mu_k) + \sum_{k\notin\mathcal{E}}(\mu_k) \\ &= \sum_{k\in\mathcal{E}}(\mu_k) + n - \operatorname{card}(\mathcal{E})\end{aligned}$$

Donc $\deg(Q) = \deg(P) - 1 = \deg(P')$.
Donc $\exists \lambda \in \mathbb{R}^*$ tel que $P = \lambda Q$ et :

$$P' = \lambda Q' = \lambda \prod_{k=1}^{n-1}(X-z_k) \prod_{k\in\mathcal{E}}(X-x_k)^{\mu_k-1}$$

▶ Polynômes irréductibles

20. *Enoncé : Décomposer en produit de facteurs irréductibles sur R les polynômes suivants :*
    (a) X^3+1 ;
    En utilisant les racines cubiques de -1 : $-1, -j, -j^2$ ou la factorisation de $a^n + b^n$ lorsque n est impair, on trouve

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

    (b) $X^8 + 1$;
    On a

    $$\begin{aligned}X^8 + 1 &= \left(X^4+1\right)^2 - 2X^4 \\ &= \left(X^4 - \sqrt{2}X^2 + 1\right)\left(X^4 + \sqrt{2}X^2 + 1\right)\end{aligned}$$

donc

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

puis.

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

Les quatre trinômes étant de discriminants strictement négatifs, ils sont irréductibles sur $\mathbb{R}$, et la décomposition sur $\mathbb{R}$ est achevée.

(c) X^4+1 ;
En appliquant les identités remarquables,

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

Les deux trinômes étant de discriminants strictement négatifs, ils sont irréductibles sur $\mathbb{R}$.

(d) X^8+X^4+1 ;

$$\begin{aligned} X^8+1X^4+1 &= \left(\mathrm{X}^4+1\right)^2-\mathrm{X}^4 \\ &= \left(\mathrm{X}^4-\mathrm{X}^2+1\right)\left(\mathrm{X}^4+\mathrm{X}^2+1\right) \end{aligned}$$

puis

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

et

$$\begin{aligned} \mathrm{X}^4+\mathrm{X}^2+1 &= \left(\mathrm{X}^2+1\right)^2-\mathrm{X}^2 \\ &= \left(\mathrm{X}^2-\mathrm{X}+1\right)\left(\mathrm{X}^2+\mathrm{X}+1\right) \end{aligned}$$

Les quatre trinômes étant de discriminants strictement négatifs, ils sont irréductibles sur $\mathbb{R}$.

(e) X^4+X^2+1 ;

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

Les deux trinômes étant de discriminants strictement négatifs, ils sont irréductibles sur $\mathbb{R}$.

(f) $X^4 - X^2 - 12$;

$$\begin{aligned} \mathrm{X}^4 - \mathrm{X}^2 - 12 &= \left(\mathrm{X}^2 - 1/2\right)^2 - \frac{49}{4} \\ &= \left(\mathrm{X}^2 - 4\right)\left(\mathrm{X}^2 + 3\right) \\ &= (\mathrm{X}-2)(\mathrm{X}+2)\left(\mathrm{X}^2 + 3\right) \end{aligned}$$

(g) $X^6 + 1$;

En utilisant la factorisation de $a^n + b^n$ lorsque n est impair, on trouve

$$X^6 + 1 = \left(\mathrm{X}^2 + 1\right)\left(\mathrm{X}^4 - \mathrm{X}^2 + 1\right)$$

Or,

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

Les deux trinômes étant de discriminants strictement négatifs, ils sont irréductibles sur $\mathbb{R}$, et la décomposition sur $\mathbb{R}$ est achevée.

(h) $X^6 - 1$;

On a

$$\begin{aligned} X^6 - 1 &= \left(X^3 - 1\right)\left(X^3 + 1\right) \\ &= (X-1)\left(X^2 + X + 1\right)(X+1)\left(X^2 - X + 1\right) \end{aligned}$$

(i) $X^{2n+1} - 1 (n \geq 1)$;

D'après le cours,

$$\begin{aligned} \mathrm{X}^{2n+1} - 1 &= \prod_{k=0}^{2n}\left(\mathrm{X} - e^{2ik\pi/(2n+1)}\right) \\ &= (\mathrm{X}-1)\prod_{k=1}^{2n}\left(\mathrm{X} - e^{2ik\pi/(2n+1)}\right) \\ &= (\mathrm{X}-1)\prod_{k=1}^{n}\left(\mathrm{X}^2 - 2\cos\frac{2k\pi}{2n+1}\mathrm{X} + 1\right) \end{aligned}$$

en regroupant les paires de racines conjuguées.

(j) $1 + X^3 + X^6 + X^9$.

On s'inspire encore de la formule de la série géométrique :

$$\left(1 - X^3\right)\left(1 + X^3 + X^6 + X^9\right) = 1 - X^{12}$$

En notant R, l'ensemble des racines douzièmes de l'unité qui ne sont pas des racines cubiques de l'unité :

$$\mathrm{R} = \left\{-1, e^{\pm i\pi/6}, e^{\pm i\pi/3}, \pm i, e^{\pm 5i\pi/6}\right\}$$

la factorisation dans $\mathbb{C}[X]$ est :

$$1 + X^3 + X^6 + X^9 = \prod_{\omega\in R} (X - \omega)$$

On associe les racines conjuguées par paires pour en déduire la factorisation dans $\mathbb{R}[\mathrm{X}]$:

$$\begin{aligned}(\mathrm{X}+1)\left(\mathrm{X}^2-\sqrt{3}\mathrm{X}+1\right)&\left(\mathrm{X}^2-\mathrm{X}+1\right)\\ &\times\left(\mathrm{X}^2+1\right)\left(\mathrm{X}^2+\sqrt{3}\mathrm{X}+1\right)\end{aligned}$$

21. *Enoncé : On pose :*

$$P = X^6 + X^5 + 3X^4 + 2X^3 + 3X^2 + X + 1.$$

(a) *Vérifier que i est racine multiple de P.*
On a :

$$\mathrm{P}(i) = \mathrm{P}'(i) = 0$$

mais

$$\mathrm{P}''(i) = -8i \neq 0$$

Le nombre i est donc une racine de P de multiplicité deux.

(b) *En déduire la décomposition de P sur R .*
Puisque P est à coefficients réels, $-i$ est également une racine de P de multiplicité deux. P est donc divisible par

$$(\mathrm{X}-i)^2(\mathrm{X}+i)^2 = \left(\mathrm{X}^2+1\right)^2$$

En posant la division euclidienne, on trouve

$$\mathrm{P} = \left(\mathrm{X}^2+1\right)^2\left(\mathrm{X}^2+\mathrm{X}+1\right)$$

Le dernier trinôme étant de discriminant strictement négatif, il est irréductible sur $\mathbb{R}$, et la décomposition de P sur $\mathbb{R}$ est finie.

22. *Enoncé : Démontrer que $X^2 + X + 1$ divise $X^8 + X^4 + 1$ dans $\mathbb{C}[X]$.*
Posons l'équation :

$$X^2 + X + 1 = 0$$

Le discriminant de l'équation est :

$$\Delta = 1^2 - 4\cdot 1\cdot 1 = 1 - 4 = -3$$

Donc les solutions sont :

$$j = \frac{-1}{2} + i\frac{\sqrt{3}}{2} = e^{i\frac{2\pi}{3}} \quad \text{et} \quad \bar{j} = \frac{-1}{2} - i\frac{\sqrt{3}}{2} = e^{-i\frac{2\pi}{3}}$$

Vérifions si j et $\bar{j}$ sont des racines de $X^8 + X^4 + 1$.

$$\begin{aligned} j^8 + j^4 + 1 &= j^6 j^2 + j^3 j + 1 \\ &= j^2 + j + 1 \\ &= 0 \end{aligned}$$

Et :

$$\begin{aligned} \bar{j}^8 + \bar{j}^4 + 1 &= \bar{j}^6 \bar{j}^2 + \bar{j}^3 \bar{j} + 1 \\ &= \bar{j}^2 + \bar{j} + 1 \\ &= 0 \end{aligned}$$

Puis les racines de $X^2 + X + 1$ sont racines de $X^8 + X^4 + 1$, alors :

$$X^2 + X + 1 \mid X^8 + X^4 + 1 \text{ dans } \mathbb{C}[X]$$

<u>Autre méthode :</u>

$$\begin{array}{rcl|l}
X^8 & +X^4 & +1 & X^2+X+1 \\ \cline{4-4}
-X^8-X^7-X^6 & & & X^6-X^5+X^3-X+1 \\ \cline{1-1}
-X^7-X^6 & & & \\
X^7+X^6+X^5 & & & \\ \cline{1-1}
X^5+X^4 & & & \\
-X^5-X^4-X^3 & & & \\ \cline{1-1}
-X^3 & & & \\
X^3+X^2+X & & & \\ \cline{1-1}
X^2+X+1 & & & \\
-X^2-X-1 & & & \\ \cline{1-1}
0 & & &
\end{array}$$

<u>Autre méthode :</u>

$$\begin{aligned} X^8 + X^4 + 1 &= (X^4+1)^2 - (X^2)^2 \\ &= (X^4 - X^2 + 1)(X^4 + X^2 + 1) \\ &= ((X^2+1)^2 - (X)^2)(X^4 + X^2 + 1) \\ &= (X^2 - X + 1)(X^2 + X + 1)(X^4 + X^2 + 1) \end{aligned}$$

23. *Enoncé : Quelle est la décomposition en produit d'irréductibles de $X^8 - 1$ dans $\mathbb{R}[X]$?*
Posons l'équation :

$$X^8 - 1 = 0$$

Posons les racines de l'équation, pour $k \in [\![0, 7]\!]$:

$$\omega_k = e^{i\frac{2k\pi}{8}}$$

Donc les racines réelles sont :

$$\omega_0 = 1 \quad \text{et} \quad \omega_4 = -1$$

et les racines complexes sont :

$$\omega_1 = e^{i\frac{\pi}{4}}, \quad \omega_2 = e^{i\frac{\pi}{2}}, \quad \omega_3 = e^{i\frac{3\pi}{4}}, \quad \omega_5 = e^{i\frac{5\pi}{4}}, \quad \omega_6 = e^{i\frac{3\pi}{2}}, \quad \omega_7 = e^{i\frac{7\pi}{4}}$$

De plus, le coefficient dominant de $X^8 - 1$ est 1.
Donc, d'après la formule du cours :

$$P = \text{cd}(P) \prod_{\alpha \in \text{Rac}_{\mathbb{R}}} (X-\alpha)^{\mu_P(\alpha)} \prod_{\beta \in \text{Rac}_{\mathbb{C}}(P) \backslash \text{Rac}_{\mathbb{R}}(P) \text{ tel que } \Im(\beta) \geq 0} (X^2 - 2\,\text{Re}(\beta)X + |\beta|^2)^{\mu_P(\beta)}$$

On regardes les racines complexes dont l'imaginaire est positif ou nul :

$$\begin{aligned}
\Im(\omega_1) &= \sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} > 0 \\
\Im(\omega_2) &= \sin\left(\frac{\pi}{2}\right) = 1 > 0 \\
\Im(\omega_3) &= \sin\left(\frac{3\pi}{4}\right) = \frac{\sqrt{2}}{2} > 0 \\
\Im(\omega_5) &= \sin\left(\frac{5\pi}{4}\right) = -\frac{\sqrt{2}}{2} < 0 \\
\Im(\omega_6) &= \sin\left(\frac{3\pi}{2}\right) = -1 < 0 \\
\Im(\omega_7) &= \sin\left(\frac{7\pi}{4}\right) = -\frac{\sqrt{2}}{2} < 0
\end{aligned}$$

Donc le résultat est :

$$\begin{aligned}
X^8 - 1 = (X-1)(X+1)(X^2 - 2\cos\left(\frac{\pi}{2}\right)X + |\omega_2|^2) \\
(X^2 - 2\cos\left(\frac{\pi}{4}\right)X + |\omega_1|^2)(X^2 - 2\cos\left(\frac{3\pi}{4}\right)X + |\omega_3|^2) \\
= (X-1)(X+1)(X^2+1)(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)
\end{aligned}$$

24. *Enoncé : Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Décomposer en produit de polynômes irréductibles dans $\mathbb{C}[\mathrm{X}]$, puis dans $\mathbb{R}[\mathrm{X}]$ le polynôme :*

$$P = X^{2n} - 2X^n \cos(n\theta) + 1$$

S'il existe $m \in \mathbb{Z}$ tel que $\theta = \frac{m\pi}{n}$, alors $\mathrm{P} = \mathrm{X}^{2n} - 2(-1)^m \mathrm{X}^n + 1$.

— Si m est pair,

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

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$. Il faut alors distinguer suivant la parité de n. Si n est pair, alors

$$\mathrm{P} = (\mathrm{X}-1)^2(\mathrm{X}+1)^2 \prod_{k=1}^{\frac{n}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{2k\pi}{n}+1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$. Si n est impair, alors

$$\mathrm{P} = (\mathrm{X}-1)^2 \prod_{k=1}^{\frac{n-1}{2}}\left(\mathrm{X}^2 - 2\cos\frac{2k\pi}{n}+1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[X]$.

— Si m est impair,

$$\mathrm{P} = (\mathrm{X}^n+1)^2 = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{\frac{(2k+1)i\pi}{n}}\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$. Il faut alors distinguer suivant la parité de n. Si n est pair, alors

$$\mathrm{P} = \prod_{k=0}^{\frac{n}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{(2k+1)\pi}{n}+1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.
Si n est impair, alors

$$\mathrm{P} = (\mathrm{X}+1)^2 \prod_{k=0}^{\frac{n-1}{2}-1}\left(\mathrm{X}^2 - 2\cos\frac{(2k+1)\pi}{n}+1\right)^2$$

qui est la décomposition en facteurs irréductibles de P dans $\mathbb{R}[\mathrm{X}]$.
Dans toutes les expressions précédentes, on convient qu'un produit indexé sur le vide vaut 1 et les facteurs sont bien irréductibles car les cosinus ne valent ni 1ni -1.
On suppose maintenant qu'il n'existe pas d'entier $m \in \mathbb{Z}$ tel que $\theta = \frac{m\pi}{n}$. Remarquons que

$$\mathrm{P} = \left(\mathrm{X}^n - e^{ni\theta}\right)\left(\mathrm{X}^n - e^{-ni\theta}\right)$$

On a

$$\mathrm{X}^n - e^{ni\theta} = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{i\left(\theta+\frac{2k\pi}{n}\right)}\right)$$

et par conjugaison

$$\mathrm{X}^n - e^{-ni\theta} = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{-i\left(\theta+\frac{2k\pi}{n}\right)}\right)$$

La décomposition de P en facteurs irréductibles dans $\mathbb{C}[X]$ est donc

$$\mathrm{P} = \prod_{k=0}^{n-1}\left(\mathrm{X} - e^{i\left(\theta+\frac{2k\pi}{n}\right)}\right)\prod_{k=0}^{n-1}\left(\mathrm{X} - e^{-i\left(\theta+\frac{2k\pi}{n}\right)}\right)$$

On en déduit que la décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$ est

$$\mathrm{P}=\prod_{k=0}^{n-1}\left(\mathrm{X}^2-2\mathrm{X}\cos\left(\theta+\frac{2k\pi}{n}\right)+1\right)$$

Les facteurs sont bien irréductibles car la condition $\theta \notin \frac{\pi}{n}\mathbb{Z}$ assure qu'aucun des cosinus ne vaut 1 ou -1 .

▶ Approfondissement

25. *Enoncé : On dit qu'un sous-groupe I de $\mathbb{K}[X]$ est un idéal si*

$$\forall P \in \mathbb{K}[X],\ \forall Q \in I, \quad PQ \in I.$$

(a) *Démontrer que, pour tout $A \in \mathbb{K}[X]$, l'ensemble $A\mathbb{K}[X]=\{AP \mid P \in \mathbb{K}[X]\}$ est un idéal de $\mathbb{K}[X]$.*
Il est clair que $A\mathbb{K}[X] \subset \mathbb{K}[X]$ et que $0=A\times 0 \in A\mathbb{K}[X]$. De plus, si P et Q sont dans $A\mathbb{K}[X]$ il existe deux polynômes U et V tels que $P=AU$ et $Q=AV$. De faite $P+Q=A(U+V) \in A\mathbb{K}[X]$: on a bien un sous-groupe de $\mathbb{K}[X]$.
Enfin, si $P=AU \in A\mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ alors $PQ=AUQ \in A\mathbb{K}[X]$, donc on a bien un idéal.

(b) *On fixe dans cette question un idéal I de $\mathbb{K}[X]$ différent de $\{0\}$.*

i. *Justifier l'existence de $r=\min\{\deg(P) \mid P \in I \setminus \{0\}\}$.*
L'ensemble considéré est une partie de $\mathbb{N}$ non vide car $I \neq \{0\}$.

ii. *Montrer qu'il existe un unique polynôme unitaire $U \in I$ de degré r.*
Il existe par construction $P \in I$ de degré r. Si on note a son coefficient dominant alors $U=\frac{1}{a}\times P \in I$ par propriété d'idéal et est unitaire de degré r.

iii. *Démontrer que $I=U\mathbb{K}[X]$.*
L'inclusion de droite à gauche est classique. Réciproquement, si $P \in I$ alors par division euclidienne il existe $Q, R \in \mathbb{K}[X]$ tels que $P=UQ+R$ et $\deg(R)<r$. Comme $R=P-UQ \in I$, il n'est pas possible que $R \neq 0$ sans contredire la minimalité de r. De fait, on a bien $P=UQ \in U\mathbb{K}[X]$.

26. *Enoncé : Soit $(P, Q) \in \mathbb{Z}[X]^2$ tel que $\gcd(P, Q)=1$. Pour $n \in \mathbb{N}$, on pose $u_n=\gcd(P(n), Q(n))$. Montrer que la suite $(u_n)_n$ est périodique.*

Puisque P et Q sont à coefficients dans $\mathbb{Z}$ et, a fortiori, à coefficients dans le corps Q , le théorème de Bézout assure l'existence de deux polynômes U et V de $\mathbb{Q}$[X] tels que $\mathrm{UP}+\mathrm{VQ}=1$. En notant d le ppcm des dénominateurs des coefficients de U et V écrits sous forme fractionnaire et en posant $\mathrm{A}=d\mathrm{U}$ et $\mathrm{B}=d$ V, on a $\mathrm{AP}+\mathrm{BQ}=d$ avec A et B dans $\mathbb{Z}$[X]. Pour tout $n \in \mathbb{N}$, $\mathrm{A}(n)\mathrm{P}(n)+\mathrm{B}(n)\mathrm{Q}(n)=d$ de sorte que u_n divise d. Montrons alors que (u_n) est d-périodique. Soit $n \in \mathbb{N}$. Pour tout $k \in \mathbb{N}$

$$(n+d)^k=n^k+\sum_{j=1}^{k}\binom{k}{j}n^{k-j}d^j=n^k+cd$$

avec $c \in \mathbb{N}$. On en déduit que $\mathrm{P}(n+d)=\mathrm{P}(n)+ad$ et $\mathrm{Q}(n+d)=\mathrm{Q}(n)+bd$ avec $(a, b) \in \mathbb{Z}^2$. Puisque u_n divise $\mathrm{P}(n), \mathrm{Q}(n)$ et d, u_n divise $\mathrm{P}(n+d)$ et $\mathrm{Q}(n+d)$ donc u_n divise u_{n+d}. De même, u_{n+d} divise $\mathrm{P}(n+d), \mathrm{Q}(n+d)$

et d de sorte que u_{n+d} divise $\mathrm{P}(n)$ et $\mathrm{Q}(n)$ et donc u_n. On en déduit que $u_{n+d} = u_n$, ce qui prouve que la suite $(u_n)_n$ est d-périodique.

27. *Enoncé : Une somme de Newton. Soient a, b, c les racines complexes du polynôme $P = X^3 - 2X + 5$.*

   (a) *Calculer $S = a^4 + b^4 + c^4$.*
   Exploitons les égalités $\mathrm{P}(a) = \mathrm{P}(b) = \mathrm{P}(c) = 0$ en effectuant la division euclidienne de X^4 par P . On trouve sans peine $\mathrm{X}^4 = \mathrm{XP} + 2\mathrm{X}^2 - 5\mathrm{X}$. Ainsi $a^4 = 2a^2 - 5a, b^4 = 2b^2 - 5b$ et $c^4 = 2c^2 - 5c$, d'où $\mathrm{S} = 2\left(a^2 + b^2 + c^2\right) - 5(a+b+c)$. Notons σ_1, σ_2 et σ_3 les fonctions symétriques d'ordre trois évaluées en a, b et c. Puisque

   $$\mathrm{P} = (\mathrm{X} - a)(\mathrm{X} - b)(\mathrm{X} - c) = \mathrm{X}^3 - \sigma_1 \mathrm{X}^2 + \sigma_2 \mathrm{X} - \sigma_3 = \mathrm{X}^3 - 2\mathrm{X} + 5$$

   on a $\sigma_1 = 0, \sigma_2 = -2$ et $\sigma_3 = -5$. Or, $\sigma_1^2 = a^2 + b^2 + c^2 + 2\sigma_2$, d'où $a^2 + b^2 + c^2 = (0)^2 - 2 \times (-2) = 4$. Ainsi, $\mathrm{S} = 2 \times 4 - 5 \times 0 = 8$.

   (b) *Trouver un polynôme de degré 3 à coefficients entiers dont a^2, b^2, c^2 sont les racines.*
   Il suffit de calculer les fonctions symétriques élémentaires en a^2, b^2 et c^2. Notons-les Σ_1, Σ_2 et Σ_3. On a clairement $\Sigma_3 = a^2b^2c^2 = (\sigma_3)^2 = 25$ et on a déjà calculé $\Sigma_1 = a^2 + b^2 + c^2 = 4$. On conclut en remarquant que

   $$\begin{aligned}\sigma_2^2 = (ab + bc + ac)^2 &= a^2b^2 + b^2c^2 + a^2c^2 + 2\left(a^2bc + ab^2c + abc^2\right) \\ &= \Sigma_2 + 2abc(a + b + c) = \Sigma_2 + 2\sigma_3\sigma_1 = \Sigma_2 + 2 \times (-5) \times 0 = \Sigma_2\end{aligned}$$

   et donc $\Sigma_2 = \sigma_2^2 = 4$. Les nombres a^2, b^2 et c^2 sont donc les racines du polynôme $\mathrm{Q} = \mathrm{X}^3 - 4\mathrm{X}^2 + 4\mathrm{X} - 25$.

28. *Enoncé :*

   (a) *Soit $n \in \mathbb{N}^*$. Factoriser sur $\mathbb{C}$ le polynôme $P_n = X^{n-1} + X^{n-2} + \cdots + X + 1$.*
   On remarque que $(\mathrm{X}-1)\mathrm{P}_n = \mathrm{X}^n - 1$ donc les racines de P_n sont les racines $n^{\text{èmes}}$ de l'unité hormis 1 . On a donc

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

   (b) *En déduire une expression simple de*

   $$A_n = \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$$

   Calculons $\mathrm{P}_n(1)$ de deux façons. D'une part, $\mathrm{P}_n(1) = n$ en utilisant l'expression de P_n donnée dans l'énoncé. D'autre part,

$$\begin{aligned}
\mathrm{P}_n(1) &= \prod_{k=1}^{n-1}\left(1-e^{\frac{2ik\pi}{n}}\right)\\
&= \prod_{k=1}^{n-1} e^{\frac{ik\pi}{n}}\left(e^{\frac{-ik\pi}{n}}-e^{\frac{ik\pi}{n}}\right)\\
&= \left(\prod_{k=1}^{n-1} e^{\frac{ik\pi}{n}}\right)\left(\prod_{k=1}^{n-1} -2i\sin\frac{k\pi}{n}\right)\\
&= e^{\frac{i\pi}{n}(1+2+\cdots+(n-1))}(-2i)^{n-1}\ \mathrm{A}_n\\
&= e^{\frac{i\pi}{n}\frac{n(n-1)}{2}}(-2)^{n-1}i^{n-1}\ \mathrm{A}_n\\
&= e^{i(n-1)\frac{\pi}{2}}(-2)^{n-1}i^{n-1}\ \mathrm{A}_n\\
&= i^{n-1}(-2)^{n-1}\ \mathrm{A}_n\\
&= \left(i^2\right)^{n-1}(-2)^{n-1}\ \mathrm{A}_n = 2^{n-1}\ \mathrm{A}_n
\end{aligned}$$

Par conséquent, $\mathrm{A}_n = \frac{n}{2^{n-1}}$.

(c) *Donner une expression simple de*

$$B_n = \prod_{k=0}^{n-1}\sin\left(\frac{k\pi}{n}+\theta\right)$$

Posons $\mathrm{Q}_n = \mathrm{X}^n - e^{2in\theta}$. Les racines de Q_n sont les $e^{2i\left(\frac{k\pi}{n}+\theta\right)}$ pour $0 \le k \le n-1$. On a donc la factorisation suivante de Q_n sur $\mathbb{C}$:

$$\mathrm{Q}_n = \prod_{k=0}^{n-1}\left(\mathrm{X}-e^{2i\left(\frac{k\pi}{n}+\theta\right)}\right)$$

D'une part, $\mathrm{Q}_n(1) = 1-e^{2in\theta}$. D'autre part,

$$\begin{aligned}
\mathrm{Q}_n(1) &= \prod_{k=0}^{n-1}\left(1-e^{2i\left(\frac{k\pi}{n}+\theta\right)}\right)\\
&= \prod_{k=0}^{n-1} e^{i\left(\frac{k\pi}{n}+\theta\right)}\left(e^{-i\left(\frac{k\pi}{n}+\theta\right)}-e^{i\left(\frac{k\pi}{n}+\theta\right)}\right)\\
&= \left(\prod_{k=0}^{n-1} e^{i\left(\frac{k\pi}{n}+\theta\right)}\right)\left(\prod_{k=0}^{n-1} -2i\sin\left(\frac{k\pi}{n}+\theta\right)\right)\\
&= \left(\prod_{k=0}^{n-1} e^{\frac{ik\pi}{n}}\right)e^{in\theta}(-2)^n i^n\ \mathrm{B}_n\\
&= i^{n-1}e^{in\theta}(-2)^n i^n\ \mathrm{B}_n = 2^{n-1}(-2i)e^{in\theta}\ \mathrm{B}_n
\end{aligned}$$

Par conséquent,

$$\mathrm{B}_n = \frac{1-e^{2in\theta}}{2^{n-1}(-2i)e^{in\theta}} = \frac{\sin n\theta}{2^{n-1}}$$

(d) *On pose* $\omega = e^{\frac{2i\pi}{n}}$. *Calculer*

$$C_n = \prod_{k=0}^{n-1} \prod_{\ell \neq k} \left(\omega^k - \omega^\ell\right)$$

$$\begin{aligned}
\mathrm{C}_n &= \prod_{k=0}^{n-1} \prod_{\substack{l=0 \\ l \neq k}}^{n-1} \left(\omega^k - \omega^l\right) \\
&= \prod_{k=0}^{n-1} \prod_{\substack{l=0 \\ l \neq k}}^{n-1} \omega^k \left(1 - \omega^{l-k}\right) \\
&= \prod_{k=0}^{n-1} \begin{pmatrix} \prod_{\substack{l=0 \\ l \neq k}}^{n-1} \omega^k \prod_{l=0}^{n-1} \left(1 - \omega^{l-k}\right) \\ l \neq k \end{pmatrix}
\end{aligned}$$

Mais, l'ensemble des ω^{l-k} pour $0 \leq l \leq n-1$ et $l \neq k$ est l'ensemble des racines $n^{\text{èmes}}$ de l'unité privé de 1 . Donc

$$\prod_{\substack{l=0 \\ l \neq k}}^{n-1} \left(1 - \omega^{l-k}\right) = \mathrm{P}_n(1) = n$$

Achevons le calcul de C_n :

$$\begin{aligned}
\mathrm{C}_n &= \prod_{k=0}^{n-1} \left(\omega^{k(n-1)} n\right) \\
&= n^n \prod_{k=0}^{n-1} \omega^{-k} \\
&= n^n \omega^{-(0+1+\cdots+(n-1))} = n^n \omega^{-\frac{n(n-1)}{2}} \\
&= n^n e^{-i(n-1)\pi} = (-1)^{n-1} n^n
\end{aligned}$$

29. *Enoncé : Soient* $a, b \in \mathbb{R}_+^*$. *Déterminer les entiers* $n \in \mathbb{N}$ *tels que* $X^2 - (a^2 + b^2)$ *divise* $X^{2n} - (a^n + b^n)^2$.
Il faut et il suffit que $\pm\sqrt{a^2 + b^2}$ soient racines de $\mathrm{X}^{2n} - (a^n + b^n)^2$, ce qui donne $(a^2 + b^2)^n = (a^n + b^n)^2$. Visiblement $n = 2$ convient mais pas 0 et 1 .

   Soit $\rho = \sqrt{a^2 + b^2}$ et $\theta \in]0, \frac{\pi}{2}[$ tel que $a + ib = \rho e^{i\theta}$. En divisant par ρ^{2n} et en prenant la racine carrée, on obtient, $1 = \cos^n \theta + \sin^n \theta$. Si $n > 2$, on a $\cos^n \theta + \sin^n \theta < \cos^2 \theta + \sin^2 \theta = 1$, puisque $\sin \theta$ et $\cos \theta$ appartiennent à $]0, 1[$. La seule solution est donc $n = 2$.

30. *Enoncé : Soient* P, Q *deux polynômes unitaires de* $\mathbb{R}[X]$ *à coefficients dans* $\mathbb{R}_+$ *tels que :*

$$PQ = \sum_{k=0}^{n-1} X^k$$

   (a) *Donner un exemple non trivial de telle décomposition.*

$$
\begin{aligned}
1+\mathrm{X}+\mathrm{X}^2+\cdots+\mathrm{X}^{n-1} &= \frac{\mathrm{X}^n-1}{\mathrm{X}-1}=\frac{(\mathrm{X}^a)^b-1}{\mathrm{X}-1} \\
&= \frac{\mathrm{X}^a-1}{\mathrm{X}-1}\left(\sum_{i=0}^{b-1}\mathrm{X}^{ai}\right)=\sum_{i=0}^{a-1}\mathrm{X}^i\times\sum_{i=0}^{b-1}\mathrm{X}^{ai}
\end{aligned}
$$

(b) *Démontrer que les coefficients de P et Q sont dans $\{0,1\}$.*

— Les racines complexes de $1+\mathrm{X}+\mathrm{X}^2+\cdots+\mathrm{X}^{n-1}$ (et donc celles de P ou Q) sont les racines n-ièmes de l'unité différentes de 1 . La seule racine réelle est -1 , si n est pair. Les facteurs du second degré de P sont de la forme $(\mathrm{X}-\alpha)(\mathrm{X}-\bar{\alpha})=\mathrm{X}^2-2\operatorname{Re}(\alpha)\mathrm{X}+1$, où α est une racine n-ième de l'unité. Comme P est unitaire, il est produit de tels facteurs avec éventuellement $X+1$ pour n pair, de sorte que le terme constant de P est égal à 1 . On remarque d'autre part que si α est racine de P, $\frac{1}{\alpha}=\bar{\alpha}$ est aussi racine de P , avec la même multiplicité égale à 1 (un tel polynôme est appelé polynôme réciproque). Les polynômes P et $\widehat{\mathrm{P}}=\mathrm{X}^{\operatorname{deg}(\mathrm{P})}\mathrm{P}\left(\frac{1}{\mathrm{X}}\right)$ ont donc les mêmes racines, toutes simples : ils sont proportionnels. Étant unitaires, ils sont égaux. Si $\mathrm{P}=\sum_{k=0}^{p}a_k\mathrm{X}^k$, où p est le degré de P , alors $\widehat{\mathrm{P}}=\sum_{k=0}^{p}a_{p-k}\mathrm{X}^k$. On en déduit que l'on a, pour tout $k\in\llbracket 0,p\rrbracket, a_{p-k}=a_k$. On obtient évidemment un résultat analogue pour le polynôme Q , dont on notera q le degré et $b_0,\ldots,b_q$ les coefficients.

— Supposons par exemple $p\leq q$. Considérons, pour $0\leq k\leq p$, le coefficient d'ordre k de PQ ; il est égal à 1 . On obtient $\sum_{i=0}^{k}a_{k-i}b_i=1$. En particulier, pour $k=p$. on a, compte tenu de la symétrie des coefficients de P ,

$$
1=\sum_{i=0}^{p}a_{p-i}b_i=\sum_{i=0}^{p}a_ib_i.
$$

Sachant que $a_0=b_0=1$ et que tous les coefficients sont positifs, on en déduit que, pour $1\leq i\leq p$, on a $a_ib_i=0$. On observe en particulier que $b_p=0$ et donc que $q>p$.

On peut ensuite montrer simplement, par récurrence sur k entier entre 0 et p, que a_k et b_k sont dans $\{0,1\}$. C'est vrai pour $k=0$ (car $a_0=b_0=1$). Si la propriété est établie jusqu'au rang $k-1$, alors

$$
a_k+b_k=a_kb_0+a_0b_k=1-\sum_{i=1}^{k-1}a_{k-i}b_i
$$

est, un entier plus petit que 1 et positif par hypothèse, donc égal à 0 ou 1. Nous avons le résultat voulu puisque nous savons que $a_k=0$ ou $b_k=0$. Considérons ensuite, pour $p+1\leq k\leq q$. le coefficient d'ordre k de PQ . On obtient $1=\sum_{i=k-p}^{k}a_{k-i}b_i$, et donc

$$
b_k=1-\sum_{i=k-p}^{k-1}a_{k-i}b_i
$$

Nous savons déjà que, pour $0\leq k\leq p$, les coefficients a_k et b_k sont dans $\{0,1\}$. Une récurrence semblable à la précédente permet de démontrer que $b_k\in\{0,1\}$, pour \$p + 1\ leq k\ leq q.\$