Fiche de TD 3

Polynômes

Correction

Exercice 1 Soient $A = X^5 + 1$ et $B = X^3 + X + 1$. On applique l'algorithme d'Euclide.

$$X^5 + 1 = (X^3 + X + 1)(X^2 - 1) - X^2 + X + 2 \tag{1}$$

$$X^3 + X + 1 = (-X^2 + X + 2)(-X - 1) + 4X + 3 \tag{2}$$

$$-X^2 + X + 2 = (4X + 3)(-\frac{X}{4} + \frac{7}{16}) \quad \underbrace{+\frac{11}{16}}_{\text{dernier reste}\neq 0} \tag{3}$$

Donc $\text{pgcd}(A, B) = +\frac{11}{16}$. Comme on prend par convention les pgcd unitaires on écrira plutôt : $\text{pgcd}(A, B) = 1$.

On a donc

$$\frac{11}{16} = -X^2 + X + 2 - (4X + 3)(-\frac{X}{4} + \frac{7}{16}) \tag{4}$$

$$= -X^2 + X + 2 - (X^3 + X + 1 - (-X^2 + X + 2)(-X - 1))(-\frac{X}{4} + \frac{7}{16}) \tag{5}$$

$$= (-X^2 + X + 2)(1 - (X + 1)(-\frac{X}{4} + \frac{7}{16})) - (X^3 + X + 1)(-\frac{X}{4} + \frac{7}{16}) \tag{6}$$

$$= (-X^2 + X + 2)(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16}) + (X^3 + X + 1)(\frac{X}{4} - \frac{7}{16}) \tag{7}$$

$$= (X^5 + 1 - (X^3 + X + 1)(X^2 - 1))(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16}) + (X^3 + X + 1)(\frac{X}{4} - \frac{7}{16}) \tag{8}$$

$$= (X^5 + 1)(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16}) + (X^3 + X + 1)(\frac{X}{4} - \frac{7}{16} - (X^2 - 1)(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16})) \tag{9}$$

$$= (X^5 + 1)(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16}) + (X^3 + X + 1)(-\frac{X^4}{4} + \frac{3X^3}{16} - \frac{5X^2}{16} + \frac{X}{16} + \frac{1}{8}) \tag{10}$$

Donc $1 = (X^5 + 1)U + (X^3 + X + 1)V$ avec :

$$U = \frac{16}{11}(\frac{X^2}{4} - \frac{3X}{16} + \frac{9}{16}) = -\frac{4X^2}{11} - \frac{3X}{11} + \frac{9}{11}$$

$$V = \frac{16}{11}(-\frac{X^4}{4} + \frac{3X^3}{16} - \frac{5X^2}{16} + \frac{X}{16} + \frac{1}{8}) = -\frac{4X^4}{11} + \frac{3X^3}{11} - \frac{5X^2}{11} + \frac{X}{11} + \frac{2}{11}$$

Exercice 2 Démontrer que pour tout corps K, l'anneau des polynômes $K[X]$ a une infinité de polynômes unitaires irréductibles.

Exercice 3 Factoriser les polynômes suivants sur $\mathbb{C}$, sur $\mathbb{R}$ et sur $\mathbb{Q}$:

$$X^4 + 1,\ X^6 + X^3 + 1,\ X^3 - 3X + 1\ .$$

Solution. **Sur $\mathbb{C}$.** On a :

$$z \in \mathbb{C},\ z^4+1=0 \Leftrightarrow z^4 \neq 1 \text{ et } \frac{z^8-1}{z^4-1}=0 \Leftrightarrow z=e^{\frac{2ik\pi}{8}}=e^{\frac{ik\pi}{4}},\ k=\pm 1 \,\text{ou}\, k=\pm 3$$

$$\Leftrightarrow z=\frac{\pm 1 \pm i}{\sqrt{2}}$$

on en déduit la factorisation dans $\mathbb{C}[X]$:

$$X^4+1=(X-\frac{1+i}{\sqrt{2}})(X-\frac{1-i}{\sqrt{2}})(X+\frac{1+i}{\sqrt{2}})(X+\frac{1-i}{\sqrt{2}}) \ .$$

Sur $\mathbb{R}$. On regroupe les facteurs $X-z$ avec leur conjugué $X-\overline{z}$ pour obtenir des polynômes réels :

$$X^4+1=\underbrace{(X-\frac{1+i}{\sqrt{2}})(X-\frac{1-i}{\sqrt{2}})}_{X^2-\sqrt{2}X+1}\underbrace{(X+\frac{1+i}{\sqrt{2}})(X+\frac{1-i}{\sqrt{2}})}_{X^2+\sqrt{2}X+1}$$

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

Ces deux facteurs sont de degré 2 et sans racines réelles donc irréductibles sur $\mathbb{R}$.

Sur $\mathbb{Q}$. Le polynôme X^4+1 est irréductible sur $\mathbb{Q}$. En effet, si $A \in \mathbb{Q}[X]$ est un polynôme unitaire tel que

$$A|X^4+1$$

dans $\mathbb{Q}[X]$, alors $A|X^4+1$ dans $\mathbb{R}[X]$ donc comme il y a unicité de la factorisation en irréductibles sur $\mathbb{R}$:

$$A|X^4+1=(X^2-\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$$

$$\Rightarrow A=1,\ \underbrace{X^2-\sqrt{2}X+1,\ X^2+\sqrt{2}X+1}_{\notin \mathbb{Q}[X]} \,\text{ou}\, (X^2-\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$$

$$\Rightarrow A=1,\ \text{ou}\, X^4+1 \ .$$

Sur $\mathbb{C}$. On a :

$$z \in \mathbb{C} \text{ et } z^6+z^3+1=0 \Leftrightarrow z^3 \neq 1 \text{ et } \frac{(z^3)^3-1}{z^3-1}=0$$

$$\Leftrightarrow z^3 \neq 1 \text{ et } \frac{z^9-1}{z^3-1}=0 \Leftrightarrow z^3 \neq 1 \text{ et } z^9=1$$

$$\Leftrightarrow z=e^{\frac{2ik\pi}{9}},\ k=\pm 1, \pm 2 \text{ou} \pm 4$$

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

$$X^6+X^3+1=(X-e^{\frac{2ik\pi}{9}})(X-e^{-\frac{2ik\pi}{9}})(X-e^{\frac{4ik\pi}{9}})(X-e^{-\frac{4ik\pi}{9}})(X-e^{\frac{8ik\pi}{9}})(X-e^{-\frac{8ik\pi}{9}})$$

Sur $\mathbb{R}$. Pour factoriser dans $\mathbb{R}[X]$, on regroupe les racines conjuguées :

$$X^6 + X^3 + 1 = (X^2 - 2\cos(\frac{2\pi}{9})X + 1)(X^2 - 2\cos(\frac{4\pi}{9})X + 1)(X^2 - 2\cos(\frac{8\pi}{9})X + 1)\ .$$

Les facteurs obtenus sont de degré 2 et irréductibles sur $\mathbb{R}$ car leurs racines sont complexes non réelles !

Sur $\mathbb{Q}$. Le polynôme $P = X^6 + X^3 + 1$ est irréductible. En effet, si

$$P = AB$$

avec $A, B \in \mathbb{Q}[X]$ deux polynômes unitaires, alors comme $\mathbb{Q}[X] \subseteq \mathbb{R}[X]$, on a forcément A et B qui sont des produits de facteurs irréductibles réels de P. Comme ces facteurs irréductibles sont de degré 2 (*cf.* plus haut), on a $\deg A, \deg B$ pairs donc puisque $\deg P = 6 = \deg A + \deg B$, on a $\{\deg A, \deg B\} = \{0, 6\}$ ou $\{2, 4\}$. La première possibilité entraîne A ou $B = 1$ et la deuxième est inpossible car si par exemple $\deg A = 2$, alors A est un des facteurs irréductibles réels de P mais les polynômes

$$X^2 - 2\cos(\frac{2\pi}{9})X + 1,\ X^2 - 2\cos(\frac{4\pi}{9})X + 1,\ X^2 - 2\cos(\frac{8\pi}{9})X + 1 \notin \mathbb{Q}[X]$$

(en effet, on peut vérifier que $2\cos(\frac{2\pi}{9})$, $2\cos(\frac{4\pi}{9})$, $2\cos(\frac{8\pi}{9})$ sont les trois racines du polynôme $X^3 - 3X + 1$. Or ce polynôme n'a pas de racines entières car ± 1 ne sont pas racines et donc n'a pas de racines rationnelles car c'est unitaire à coefficients entiers !)

Le polynôme $X^3 - 3X + 1$ a trois racines réelles

$$2\cos(\frac{2\pi}{9}),\ 2\cos(\frac{4\pi}{9}),\ 2\cos(\frac{8\pi}{9})$$

(en effet $(2\cos x)^3 - 3.(2\cos x) = 2\cos(3x) \Rightarrow (2\cos x)^3 - 3.(2\cos x) = -1$ si $x = \frac{2\pi}{9}, \frac{4\pi}{9}, \frac{8\pi}{9}$).

Donc sur $\mathbb{R}$ et sur $\mathbb{C}$, on a la factorisation :

$$X^3 - 3X + 1 = (X - 2\cos(\frac{2\pi}{9}))(X - 2\cos(\frac{4\pi}{9}))(X - 2\cos(\frac{8\pi}{9}))\ .$$

Sur $\mathbb{Q}$. Le polynôme $X^3 - 3X + 1$ est irréductible car de degré 3 et sans racine rationnelle.

(En effet, si $\deg P = 3$ et si $P = AB$ alors $3 = \deg AB = \deg A + \deg B \Rightarrow \{\deg A, \deg B\} = \{0, 3\}$ ou $\{1, 2\}$ mais un polynôme de degré 1 a toujours une racine ! [†])

Exercice 4 Trouver un polynôme rationnel de degré 4 qui annule $\sqrt{2} + \sqrt{3}$. Le factoriser sur $\mathbb{R}$.

Solution. Soit $\alpha = \sqrt{2} + \sqrt{3}$. On a :

$$\alpha^2 = 5 + 2\sqrt{6} \tag{11}$$

$$\Rightarrow (\alpha^2 - 5)^2 = 24 \tag{12}$$

$$\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0\ . \tag{13}$$

†. Si $a \neq 0$, $-\frac{b}{a}$ est la racine du polynôme $aX + b$

Donc le polynôme $P(X) = X^4 - 10X^2 + 1$ convient. On vérifie que ses autres racines sont

$$\pm\sqrt{2} \pm \sqrt{3}$$

donc

$$P(X) = (X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3}) \ .$$

Exercice 5 Polynômes cyclotomiques

Soit $n \geqslant 1$. On pose

$$\Phi_n(X) = \prod_{\substack{k=1 \\ \mathrm{pgcd}(k,n)=1}}^{n} (X - e^{\frac{2ik\pi}{n}}) \ .$$

a) Calculer $\Phi_1(X)$, $\Phi_2(X)$, $\Phi_3(X)$, $\Phi_4(X)$, $\Phi_5(X)$.

Solution. On a :

$$\Phi_1(X) = X - 1,\ \Phi_2(X = X + 1),\ \Phi_3(X) = X^2 + X + 1,$$

$$\Phi_4(X) = X^2 + 1,\ \Phi_5(X) = X^4 + X^3 + X^2 + X + 1 \ .$$

b) Montrer que $\displaystyle\prod_{d|n} \Phi_d(X) = X^n - 1$.

Solution.

Soit $E = \{\frac{1}{n}, \frac{2}{n}, ..., \frac{n-1}{n}, \frac{n}{n}\}$. Chaque fraction de l'ensemble E a une unique forme irréductible $\frac{k}{d}$ avec $1 \leqslant k \leqslant d$, $k \wedge d = 1$, $d|n$.

On obtient une réunion disjointe :

$$E = \bigsqcup_{d|n} \left\{ \frac{k}{d} \ : \ 1 \leqslant k \leqslant d,\ k \wedge d = 1 \right\}$$

On en déduit :

$$X^n - 1 = \prod_{x \in E} (X - e^{2i\pi x}) = \prod_{d|n} \underbrace{\prod_{\substack{k=1 \\ k \wedge d=1}}^{d} (X - e^{\frac{2ik\pi}{d}})}_{\Phi_d(X)}$$

c) En déduire par récurrence sur $n \geqslant 1$ que $\Phi_n(X) \in \mathbb{Z}[X]$. *Solution.* Il est clair que les polynômes $\Phi_n(X)$ sont unitaires. On démontre par récurrence sur $n \geqslant 1$ que :

$$(H_n)\ \forall\, 1 \leqslant k \leqslant n,\ \Phi_k(X) \in \mathbb{Z}[X] \ .$$

Si $n = 1$, (H_1) est vraie car $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

On suppose que $(H_{n-1}$ est vraie, $n \geqslant 2$ et on montre (H_n).

Par hypothèse de récurrence (H_{n-1}) on a :

$$\forall\, d < n,\ \Phi_d(X) \in \mathbb{Z}[X]$$

donc le polynôme

$$B = \prod_{\substack{d|n \\ d<n}} \Phi_d(X)$$

est unitaire à coefficients entiers.

On peut faire la division euclidienne de $X^n - 1$ par B dans $\mathbb{Q}[X]$:

$$X^n - 1 = BQ + R \tag{14}$$

pour un unique couple (Q, R) de polynômes $\in \mathbb{Q}[X]$.

Or, comme B est unitaire, le résultat de la division euclidienne reste dans $\mathbb{Z}[X]$. †

On peut aussi faire la division euclidienne dans $\mathbb{C}[X]$:

$$X^n - 1 = B\Phi_n(X)\ .$$

Par unicité de la division euclidienne, on a forcément :

$$\Phi_n(X) = Q$$

donc $\Phi_n(X) \in \mathbb{Z}[X]$. Cela termine la récurrence.

d) En déduire aussi la formule : $\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(\frac{n}{d})}$ où μ est la fonction de Möbius.

Solution. On rappelle la définition de la fonction de Möbius.

Si $n = p_1 \ldots p_r$ avec $p_1, \ldots, p_r$ des nombres premiers (positifs) deux à deux distincts, on pose $\mu(n) = (-1)^r$. On pose $\mu(n) = 0$ dans tous les autres cas.

Par exemple $\mu(1) = 1, \mu(2) = -1, \mu(6) = 1, \mu(9) = 0$.

On calcule.

$$\prod_{d|n}(X^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n}\left(\prod_{k|d}\Phi_k(X)\right)^{\mu(\frac{n}{d})} \tag{15}$$

$$= \prod_{k|n}\prod_{\substack{d \\ k|d|n}} \Phi_k(X)^{\mu(\frac{n}{d})} \tag{16}$$

$$= \prod_{k|n}\Phi_k(X)^{\sum_{\substack{d \\ k|d|n}} \mu(\frac{n}{d})} \tag{17}$$

†. car dans $\mathbb{Z}$ tout entier est divisible par 1.

On peut faire le changement de variable $e = \frac{d}{k}$.

(18) $$\prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})} = \prod_{k|n}\Phi_k(X)^{\sum_{e|\frac{n}{k}}\mu(\frac{\frac{n}{k}}{e})}$$

or, pour tout entier l, on a $\sum_{e|l}\mu(\frac{l}{e}) = \begin{cases} 1 & \text{si } l=1 \\ 0 & \text{sinon} \end{cases}$ †

donc :

(19) $$\forall\, k|n,\ \sum_{e|\frac{n}{k}}\mu(\frac{\frac{n}{k}}{e}) = \begin{cases} 1 & \text{si } k=n \\ 0 & \text{sinon.} \end{cases}$$

d'où :

(20) $$\prod_{d|n}(X^d-1)^{\mu(\frac{n}{d})} = \Phi_n(X)\ .$$

Exercice 6 Soient $m, n \in \mathbb{Z}$. Montrer que

$$\mathrm{pgcd}(X^m-1, X^n-1) = X^{\mathrm{pgcd}(m,n)}-1$$

a) en factorisant en produit de polynômes irréductibles dans $\mathbb{C}[X]$;

Solution. Posons $\boldsymbol{\mu}_n = \{z \in \mathbb{C} : z^n = 1\}$ pour tout $n \geqslant 1$.

En factorisant dans $\mathbb{C}[X]$, on a :

$$X^n - 1 = \prod_{z\in\boldsymbol{\mu}_n}(X-z) \text{ et } X^m-1 = \prod_{z\in\boldsymbol{\mu}_m}(X-z)$$

donc

$$\mathrm{pgcd}(X^m-1, X^n-1) = \prod_{z\in\boldsymbol{\mu}_m\cap\boldsymbol{\mu}_n}(X-z)\ .$$

Or, $\boldsymbol{\mu}_m \cap \boldsymbol{\mu}_n = \mu_d$ où $d = \mathrm{pgcd}(m,n)$ ‡

Donc

$$\mathrm{pgcd}(X^m-1, X^n-1) = \prod_{z\in\boldsymbol{\mu}_d}(X-z) = X^d-1\ .$$

†. En effet, si $l = p_1^{\alpha_1}....p_r^{\alpha_r}$ pour un entier $r \in \mathbb{N}$, des nombres premiers deux à deux distincts p_i et des exposants $\alpha_i \in \mathbb{N}_{>0}$, on a

$$\begin{aligned}\sum_{e|l}\mu(\frac{l}{e}) &= \sum_{0\leqslant k\leqslant r}\ \sum_{1\leqslant i_1<\ldots<i_k\leqslant r}\mu(p_{i_1}...p_{i_k}) \\ &= \sum_{0\leqslant k\leqslant r}\binom{r}{k}(-1)^k = (1-1)^r = 0^r\end{aligned}$$

$= 0$ si $r > 0$ ...

‡. En effet, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = d$ donc $z^m = z^n = 1 \Rightarrow z^d = z^{mu+nv} = (z^m)^u(z^n)^v = 1$; la réciproque est évidente car $d|m$ et $d|n$.

b) avec l'algorithme d'Euclide.

Solution. On montre par récurrence sur $n \geqslant 1$ que

$$(H_n)\ \forall\, m \geqslant 1,\ \forall\, 1 \leqslant k \leqslant n,\ \mathrm{pgcd}(X^m - 1, X^k - 1) = X^{\mathrm{pgcd}(m,k)} - 1\ .$$

Initialisation. Si $n = 1$, (H_1) est vraie car $X - 1 | X^m - 1$ pour tout m.

Supposons (H_{n-1}) pour un $n \geqslant 2$. Montrons (H_n).

La division euclidienne de m par n donne :

$$m = nq + r$$

avec $q \in \mathbb{N}$ et $0 \leqslant r < n$. Si $r = 0$, alors $n|m$ et

$$X^m - 1 = (X^n - 1)(1 + X^n + ... + (X^n)^{\frac{n}{m}-1}) \tag{21}$$
$$\Rightarrow X^n - 1 | X^m - 1 \tag{22}$$
$$\Rightarrow \mathrm{pgcd}(X^m - 1, X^n - 1) = X^n - 1\ . \tag{23}$$

Si $1 \leqslant r \leqslant n-1$, alors $\mathrm{pgcd}(m,n) = \mathrm{pgcd}(n,r)$ donc par hypothèse de récurrence (H_{n-1}), $\mathrm{pgcd}(X^n - 1, X^r - 1) = X^{\mathrm{pgcd}(n,r)} - 1$.

Or, on a :

$$X^m - 1 = X^m - X^r + X^r - 1 \tag{24}$$
$$= X^r(X^{qn} - 1) + X^r - 1 \tag{25}$$
$$= X^r(1 + X^n + ... + (X^n)^{q-1})(X^n - 1) + X^r - 1\ . \tag{26}$$

Donc comme $r < n$, $X^r - 1$ est le reste de la division euclidienne de $X^m - 1$ par $X^n - 1$.

Donc

$$\mathrm{pgcd}(X^m - 1, X^n - 1) = \mathrm{pgcd}(X^n - 1, X^r - 1) \tag{27}$$
$$= X^{\mathrm{pgcd}(n,r)} - 1 \tag{28}$$
$$= X^{\mathrm{pgcd}(m,n)} - 1\ . \tag{29}$$

Exercice 7 Polynômes de Tchebychev

a) On définit par récurrence :

$$T_0(X) = 1,\ T_1(X) = X,\ T_{n+1}(X) = 2XT_n(X) - T_{n-1}(X) \in \mathbb{Z}[X]\ .$$

Calculer $T_2(X)$, $T_3(X)$, $T_4(X)$.

b) Montrer que $\forall\, n \geqslant 0$, $\forall\, t \in \mathbb{R}$, $T_n(\cos t) = \cos nt$ et en déduire les racines de T_n.

c) En déduire que $\forall\, m, n \geqslant 1$, $T_n \circ T_m = T_m \circ T_n$.

d) Montrer que

$$\forall\, n \geqslant 1, \forall\, t \in \mathbb{R},\ \sin nt = U_n(\cos t)\sin t$$

où si $n \geqslant 1$, $U_n(X) = \frac{T_n'(X)}{n}$.

Exercice 8 Critère d'Eisenstein

a) Soient $A, B \in \mathbb{Z}[X]$. Soit p un nombre premier. Montrer que si p divise tous les coefficients du polynôme AB, alors p divise tous les coefficients de A ou bien tous les coefficients de B. *Indication. Vérifier que dans l'anneau* $\mathbb{Z}/p\mathbb{Z}[X]$, $\overline{A}\,\overline{B} = 0 \Rightarrow \overline{A}$ *ou* $\overline{B} = 0$.

b) Si $P \in \mathbb{Z}[X]$, on note $c(P)$ le pgcd de tous les coefficients du polynôme P. En déduire le lemme de Gauss suivant.

Lemme. Soient $A, B \in \mathbb{Z}[X]$. On a $c(AB) = c(A)c(B)$.

c) Soit $P(X) = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :

(i) $p | a_0, \ldots, a_{n-1}$;

(ii) $p \nmid a_n$;

(iii) $p^2 \nmid a_0$.

Montrer que P est irréductible sur $\mathbb{Q}$.

d) En déduire pour tout $n \geqslant 1$ un polynôme irréductible sur $\mathbb{Q}$.

Exercice 9 Polynômes à valeurs entières

Si $k \in \mathbb{N}$, on pose

$$\binom{X}{k} = \frac{X(X-1)\ldots(X-k+1)}{k!} \in \mathbb{Q}[X] \ .$$

a) Montrer que

$$\forall\, k \in \mathbb{N},\ \binom{X+1}{k} - \binom{X}{k} = \binom{X}{k-1} \ .$$

Solution. Le polynôme de gauche et celui de droite sont de degré $\leqslant k-1$ et ont au moins k racines communes :

$$0, \ldots, k-1 \ .$$

Donc ils sont égaux !

b) Montrer que

$$\forall\, k \in \mathbb{N},\ \forall\, n \in \mathbb{Z},\ \binom{X}{k}(n) \in \mathbb{Z}\ ^{\dagger}$$

Solution. On a $\binom{X}{k}(n) = \binom{n}{k}$ si $n \in \mathbb{N}$ et $\pm\binom{-n+k-1}{k}$ si $n < 0$.

c) Si $f : \mathbb{N} \to \mathbb{R}$ est une fonction, on pose

$$\Delta f : n \mapsto f(n+1) - f(n)$$

et on définit par récurrence

$$\forall\, k \geqslant 1,\ \Delta^k f = \Delta\Delta^{k-1} f\ .$$

Soit $d \in \mathbb{N}$. Montrer qu'une fonction $f : \mathbb{N} \to \mathbb{R}$ est polynomiale de degré d en n si et seulement si $\Delta^{d+1} f = 0$. *Indication. Raisonner par récurrence sur $d \geqslant 0$.*

Solution. Si f est polynomiale, alors Δf aussi et on a $\deg \Delta f \leqslant \deg f - 1$. On en déduit que si f est de degré $\leqslant d$, $\deg \Delta^{d+1} f < 0 \Rightarrow \Delta^{d+1} f = 0$. Réciproquement, on raisonne par récurrence sur $d \geqslant 0$; Si $d = 0$, $\Delta f = 0 \Rightarrow \forall\, n,\ f(n+1) = f(n) \Rightarrow f$ constante donc polynomiale de degré 0. Supposons que $\Delta^d f = 0 \Rightarrow f$ polynomiale de degré $\leqslant d-1$ pour toute fonction f, pour un certain $d \geqslant 1$. Soit f une fonction telle que $\Delta^{d+1} f = 0$. Alors par hypothèse de récurrence, Δf est polynomiale de degré $\leqslant d-1$. Or les polynômes $\binom{X}{k}$, $0 \leqslant k \leqslant d-1$ forment une base de l'espace des fonctions polynomiales réelles de degré $\leqslant d-1$. Donc il existe des coefficients réels $c_1, \ldots, c_d$ tels que

$$\Delta f = c_1\binom{X}{0} + \ldots + c_d\binom{X}{d-1}\ .$$

Or, d'après a), $\forall\, k \geqslant 1$, $\binom{X}{k-1} = \Delta\binom{X}{k}$ donc :

$$\Delta f = \Delta\left(c_1\binom{X}{1} + \ldots + c_d\binom{X}{d}\right)$$

par linéarité de l'opérateur Δ. Donc $f - c_1\binom{X}{1} + \ldots + c_d\binom{X}{d} =$ *constante* donc f est bien polynomiale de degré $\leqslant d$. Cela termine la récurrence.

d) En déduire que $\sum_{k=0}^{n-1} k^d$ est un polynôme de degré $d+1$ en n.

e) Soit $f : \mathbb{N} \to \mathbb{R}$ une fonction polynomiale de degré d. On suppose que

$$f(0),\ f(1),\ \ldots,\ f(d) \in \mathbb{Z}\ .$$

Montrer qu'il existe des entiers $c_0, \ldots, c_d \in \mathbb{Z}$ tels que

$$f = c_0\binom{X}{0} + \ldots + c_d\binom{X}{d}\ .$$

†. bien que $\binom{X}{k} \notin \mathbb{Z}[X]$ si $k \geqslant 2$.

En particulier $\forall\, n \in \mathbb{N},\ f(n) \in \mathbb{Z}$.[†] *Indication. Vérifier que* $\forall\, 0 \leqslant k \leqslant d,\ c_k = \Delta^k f(0)$.

Solution. D'après a), $\forall\, j \geqslant k$, $\Delta^k\binom{X}{j} = \binom{X}{j-k}$ donc $\Delta^k\binom{X}{k} = 1$ et $\forall\, j > k$, $\Delta^k\binom{X}{j}(0) = \binom{X}{j-k}(0) = 0$.

Comme $\Delta^k\binom{X}{j} = 0$ si $j < k$, on en déduit facilement le résultat par linéarité de l'opérateur Δ.

f) Trouver les coefficients pour $\sum_{k=0}^{n-1} k^2$ et $\sum_{k=0}^{n-1} k^3$. En déduire :

$$\sum_{k=0}^{n-1} k^2 = \frac{(n-1)n(2n-1)}{6},\ \sum_{k=0}^{n-1} k^3 = \binom{n}{2}^2 .$$

Solution. Par exemple si $F(n) = \sum_{k=0}^{n-1} k^3$, on a le tableau suvant de valeurs des $\Delta^k F(n)$, $0 \leqslant k \leqslant 4$, $0 \leqslant n \leqslant 4$:

n	0	1	2	3	4
$F(n)$	0	0	1	9	36
$\Delta F(n)$	0	1	8	27	
$\Delta^2 F(n)$	1	7	19		
$\Delta^3 F(n)$	6	12			
$\Delta^4 F(n)$	6				

Donc $F(n) = \binom{n}{2} + 6\binom{n}{3} + 6\binom{n}{4} = \binom{n}{2}^2$.

g) On suppose que f est un polynôme réel ou complexe. On suppose que

$$\forall\, n >> 0,\ f(n) \in \mathbb{Z}$$

Montrer que $f(n) \in \mathbb{Z}$ pour tout n. *Indication. Raisonner avec* $f(X+a)$ *où* a *est un entier assez grand !*

Exercice 10 Méthode de Cardan pour les équations de degré 3

Soient $p, q \in \mathbb{C}$. Soit $P(X) = X^3 + pX + q \in \mathbb{C}[X]$.

a) Vérifier que si u, v vérifient $(*)$ $\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \end{cases}$, alors $x = u+v$ est racine du polynôme P.

b) Soient u, v des racines cubiques :

$$u := \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}},\ v := \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

†. Et si f est définie et polynomiale sur $\mathbb{Z}$, $\forall\, n \in \mathbb{Z},\ f(n) \in \mathbb{Z}$.

telles que $uv = -\frac{p}{3}$.

Justifier que c'est possible et déduire de la question précédente que les racines de P sont : $u+v,\ ju+j^2v,\ j^2u+jv$.

c) **Applications.** En déduire les formules suivantes :

$$\sqrt[3]{\frac{-1+\frac{1}{3}\sqrt{\frac{31}{3}}}{2}}+\sqrt[3]{\frac{-1-\frac{1}{3}\sqrt{\frac{31}{3}}}{2}} \text{ est l'unique racine réelle de } X^3+X+1$$

$$2\cos\frac{2\pi}{9} = \sqrt[3]{-\frac{1}{2}+i\frac{\sqrt{3}}{2}}+\sqrt[3]{-\frac{1}{2}-i\frac{\sqrt{3}}{2}}$$

$$2\cos\frac{2\pi}{7} = -\frac{1}{3}+\frac{1}{3}\left(\sqrt[3]{\frac{7+21i\sqrt{3}}{2}}+\sqrt[3]{\frac{7-21i\sqrt{3}}{2}}\right)$$

Indication. Utiliser la formule $2\cos(3x) = (2\cos x)^3 - 3.(2\cos x)$.

Exercice 11 Méthode d'Euler pour les équations de degré 4

Soient $p, q, r \in \mathbb{C}$. Soit $P(X) = X^4 + pX^2 + qX + r \in \mathbb{C}[X]$.

a) Vérifier que si u, v, w vérifient :

$$(*) \begin{cases} u+v+w = -p/2 \\ \sqrt{u}\sqrt{v}\sqrt{w} = -q/8 \\ -(u+v+w)^2 + 4(uv+uw+vw) = -r \end{cases}$$

alors $x = \sqrt{u}+\sqrt{v}+\sqrt{w}$ est racine du polynôme P.

b) En déduire que si u, v, w sont les trois racines du polynôme :

$$T^3 + \frac{p}{2}T^2 + (\frac{(p/2)^2-r}{4})T - \left(\frac{q}{8}\right)^2$$

et si on choisit des racines carrées telles que

$$\sqrt{u}\sqrt{v}\sqrt{w} = -q/8$$

(justifier que c'est possible), alors les racines du polynôme P sont :

$$\sqrt{u}+\sqrt{v}+\sqrt{w}\,,\ \sqrt{u}-\sqrt{v}-\sqrt{w}\,,\ -\sqrt{u}+\sqrt{v}-\sqrt{w}\,,\ -\sqrt{u}-\sqrt{v}+\sqrt{w}\ .$$

c) **Application.** *Seulement pour les calculateurs motivés :* trouver les racines du polynôme $X^4 - X - 1$.