Polynômes

Marc SAGE

18 décembre 2005

Table des matières

Profitons de cette feuille d'exercice sur les polynômes pour rappeler que l'adjectif "polynomial" *ne prend pas* d'accent circonflexe, contrairement au nom associé...

1 En apéritif

a) *Calculer le reste de la division euclidienne de* $((\sin\theta)X+\cos\theta)^n$ *par* X^2+1.

b) *Soit* P *un polynôme unitaire non constant scindé simple sur* $\mathbb{Z}$. *Montrer que* $P-1$ *est irréductible sur* $\mathbb{Z}[X]$.

c) *Soit* $a_1,...,a_n$ *et* $b_1,...,b_n$ *des réels tous distincts. On met dans un tableau* $n\times n$ *le nombre* $c_{i,j}=a_i+b_j$ *à l'intersection de la* i*-ième ligne et de la* j*-ième colonne. Montrer que si le produit* $\prod_j c_{i,j}$ *des* $c_{i,j}$ *sur une ligne donnée ne dépend pas de la ligne choisie, alors il en est de même pour le produit* $\prod_i c_{i,j}$ *sur une colonne quelconque.*

Solution proposée.

a) Soit $aX+b$ le reste cherché :

$$((\sin\theta)X+\cos\theta)^n=\left(X^2+1\right)(*)+aX+b.$$

Évaluant en $\pm i$ on obtient $e^{\pm ni\theta}=\pm ai+b$, d'où $\left\{\begin{array}{l} a=\sin n\theta \\ b=\cos n\theta \end{array}\right.$.

b) Par hypothèse, $P-1$ s'écrit sous la forme $\prod_{i=1}^n(X-a_i)-1$ où les a_i sont entiers et distincts. Supposons par l'absurde que $P-1$ se casse en un produit AB de deux polynômes à coefficients entiers de degré $<n$. On a alors

$$A(a_i)B(a_i)=AB(a_i)=-1,$$

et comme $A(a_i)$ et $B(a_i)$ sont entiers, ils valent chacun ±1 et sont opposés, ce qui montre que $A+B$ s'annule en les a_i, d'où $A+B=0$ en prenant les degrés (trop de racines). On en déduit $P=1+AB=1-A^2$ dont le coefficient dominant est négatif si $\deg A\geq 1$, ce qui contredit l'uniatarité de P. Il en résulte A constant et $P=1-A^2$ constant, *absurde.*

c) Notons $\gamma=\prod_j c_{i,j}$ le produit commun sur une colonne. En introduisant le polynôme

$$P=\prod_{j=1}^n(X+b_j)-\gamma,$$

les hypothèses montrent que les a_i sont racines de P, et on les a toutes puisque les a_i sont distincts et $\deg P=n$. On en déduit $P=\prod_{i=1}^n(X-a_i)$, ce qui évalué en $X=-b_j$ donne

$$\begin{aligned} 0-\gamma &= \prod_{i=1}^n(-b_j-a_i) \\ \gamma(-1)^{n+1} &= \prod_{i=1}^n c_{i,j}, \end{aligned}$$

d'où le résultat puisque j est pris quelconque.

Remarque. L'hypothèse "les a_i sont tous distincts" est vitale pour le troisième point : considérer le contre-exemple $a_1=a_2=b_1=0$ et $b_1=1$, qui donne le tableau

$$\left[\begin{array}{cc} 0 & 1 \\ 0 & 1 \end{array}\right].$$

2 Un corps fini n'est jamais algébriquement clos

On rappelle qu'un corps K est algébriquement clos si tout polynôme non constant de $K[X]$ admet au moins une racine dans K.

Montrer qu'un corps fini n'est jamais algébriquement clos.

Solution proposée.
Soit $K = \{\lambda_1, ..., \lambda_n\}$ un tel corps. Le polynôme

$$\prod_{i=1}^{n}(X - \lambda_i) + 1$$

de $K[X]$ n'a alors aucune racine dans K : il vaut 1 partout.

3 Invariance des pgcd et ppcm par extension de corps

Soit A et B deux polynômes de $K[X]$ où K est un corps. On considère $K \subset L$ une extension de K, et on note $\widetilde{A}$ et $\widetilde{B}$ les polynômes A et B plongés dans $L[X]$ (penser à $\mathbb{R} \subset \mathbb{C}$).
Montrer que les pgcd $A \wedge B$ et $\widetilde{A} \wedge \widetilde{B}$ coïncident, au sens où

$$\widetilde{A} \wedge \widetilde{B} = \widetilde{A \wedge B}$$

De même pour les ppcm.

Solution proposée.
Le pgcd s'obtenant par l'algorithme d'Euclide qui est une suite de divisions euclidiennes, il suffit de montrer que le quotient et le reste d'une division euclidienne $A = BQ + R$ sont inchangés par extension de corps. Or, ceci découle de leur unicité : si $A = BQ + R$ dans $K[X]$, on plonge le tout dans $L[X]$, ce qui fournit l'unique $\left(\widetilde{Q}, \widetilde{R}\right)$ de la division euclidienne $\widetilde{A} = \widetilde{B}\widetilde{Q} + \widetilde{R}$.
Pour le ppcm, on remarque que $(A \wedge B)(A \vee B) = AB$ et on applique ce qui précède.

4 Les fonctions trigonométriques ne sont pas des polynômes

Montrer que les fonctions cos, sin *et* tan *ne sont pas des polynômes.*

Solution proposée.
Sthûsss : on dérive.
Si cos vaut un certain P, alors $P \neq 0$ car cos n'est pas nul partout, donc $P \neq P''''$; or $\cos'''' = \cos$... Idem pour sin. Pour tan, le polynôme P hypothétique devrait vérifier $P' = 1 + P^2$, ce qui commence à poser problème quand on prend les degrés.

5 Le polynôme tronqué de l'exponentielle à un ordre pair n'a pas de racines réelles

Montrer que le polynôme $1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + ... + \frac{X^{2n}}{(2n)!}$ n'a pas de racines réelles.

Solution proposée.
Le terme dominant étant positif, on demande en fait de montrer que notre polynôme P reste strictement positif. En notant m l'infimum de P, il s'agit de montrer $m > 0$.

Un truc sympathique avec l'exponentielle, c'est son comportement lorsqu'on la dérive ; cela doit nous inciter à dériver P, ce qui donne

$$P = P' + \frac{X^{2n}}{(2n)!}.$$

Ainsi, si m est atteint en un réel a, on aura

$$P \geq m = P(a) = \underbrace{P'(a)}_{=0} + \underbrace{\frac{a^{2n}}{(2n)!}}_{\geq 0} \geq 0$$

avec égalité seulement $a = 0$, mais alors $P'(a) = P'(0) = 1$ (ce qui est exclu), d'où le résultat. Il s'agit donc de montrer que m est atteint.

P étant de degré pair, il a pour limite ∞ en $\pm\infty$, donc il y a segment $[-A, A]$ en-dehors duquel $|P| > m+1$; l'infimum de P peut par conséquent être pris sur le segment $[-A, A]$, où l'on sait que toute application continue (a *fortiori* P) va atteindre ses bornes. Ploum.

6 Un exercice d'interpolation

Soit P un polynôme de degré $\leq n$ tel que $P(i) = \frac{1}{\binom{n+1}{i}}$ pour tout $i = 0, ..., n$. Calculer $P(n+1)$.

Solution proposée.

On utilise la formule d'interpolation de Lagrange

$$P(x) = \sum_{i=0}^{n} P(i) \prod_{j \neq i} \frac{x-j}{i-j}$$

que l'on évalue en $x = n+1$. On a déjà

$$\begin{aligned}\prod_{j \neq i} \frac{(n+1)-j}{i-j} &= \frac{n+1}{i}\frac{n}{i-1}...\frac{n-i+2}{1} \times \frac{n-i}{-1}\frac{n-i-1}{-2}...\frac{1}{-(n-i)} \\ &= \frac{(n+1)!}{n-i+1}\frac{(-1)^{n-i}}{i!\,(n-i)!} = (-1)^{n-i}\binom{n+1}{i},\end{aligned}$$

d'où

$$P(n+1) = \sum_{i=0}^{n} (-1)^{n-i} = \begin{cases} 0 \text{ si } n \text{ pair} \\ 1 \text{ si } n \text{ impair} \end{cases}.$$

7 Tout polynôme réel positif est somme de deux carrés

Soit P un polynôme à coefficients réels qui est toujours positif. Montrer que P s'écrit comme la somme $A^2 + B^2$ de deux carrés de polynômes.

Solution proposée.

L'idée est que, P ne changant pas de signe, tout facteur $X - \lambda$ le divisant doit apparaître un nombre pair de fois (sinon P change de signe autour de λ). Quant aux racines complexes, elles sont deux à deux conjuguées car P est à coefficients réels. On peut donc casser P dans $\mathbb{C}$ sous la forme

$$P = \prod (X - \lambda_i)^2 \prod (X - \xi_j)(X - \overline{\xi_j}).$$

Un oeil aguerri (ou pas) réécrira cela sous la forme

$$P = Q\overline{Q} \text{ avec } Q = P = \prod (X - \lambda_i) \prod (X - \xi_j).$$

Il suffit de faire apparaître les parties réelle et imaginaire de $Q = A + Bi$ pour conclure :

$$P = Q\overline{Q} = (A + iB)(A - iB) = A^2 + B^2.$$

8 Calculer sans se fatiguer

On se donne quatre réels a, b, c, d vérifiant

$$\begin{cases} a = \sqrt{4 - \sqrt{5 - a}} \\ b = \sqrt{4 + \sqrt{5 - b}} \end{cases} \begin{cases} c = \sqrt{4 - \sqrt{5 + c}} \\ d = \sqrt{4 + \sqrt{5 + d}} \end{cases}.$$

Calculer le produit $abcd$.

Solution proposée.
L'idée est d'introduire un polynôme dont a, b, c, d seraient les racines, et de prendre son terme constant (qui vaut $abcd$).

Les nombres a et b sont racines de $\left(X^2 - 4\right)^2 = 5 - X$, ce qui se réécrit $X^4 - 8X^2 + X + 11$. De même, c et d sont racines de $X^4 - 8X^2 - X + 11$. La différence entre les deux polynômes ne tenant qu'à un signe devant l'unique puissance impaire X, il suffit de changer c et d en leurs opposés, ce qui fournit les quatre racines du polynôme $X^4 - 8X^2 + X + 11$, d'où le produit cherche $abcd = 11$.

Il reste toutefois à vérifier que $a, b, -c, -d$ sont distincts. Si jamais $a = b$, alors

$$4 - \sqrt{5 - a} = a^2 = b^2 = 4 + \sqrt{5 - b} = 4 + \sqrt{5 - a}$$
$$\Longrightarrow a = 5 \Longrightarrow a = \sqrt{4 - \sqrt{5 - 5}}, \textit{ absurde.}$$

Les autres cas se traitent de manière analogue.

9 Une fonction localement polynomiale est un polynôme

Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une application localement polynomiale, i.e. *vérifiant*

$$\forall a \in \mathbb{R},\ \exists \varepsilon > 0,\ \exists P \in \mathbb{R}[X],\ f = P \textit{ sur }]a - \varepsilon, a + \varepsilon[.$$

Montrer qu'en fait f est un polynôme.

Solution proposée.
On sait déjà que f vaut un certain polynôme P sur un $[0, \varepsilon[$ avec $\varepsilon > 0$. L'idée est de pousser le plus loin possible le ε tout en conservant $f = P$ sur $[0, \varepsilon[$. On introduit par conséquent

$$\alpha = \sup \{\varepsilon > 0 \ ;\ f = P \text{ sur } [0, \varepsilon[\} \in \mathbb{R}^+ \cup \{\infty\}$$

et on va montrer que nécessairement $\alpha = \infty$.

Si ce n'est pas le cas, $\alpha \in \mathbb{R}$, et par hypothèse f vaut un certain polynôme Q sur $]\alpha - \delta, \alpha + \delta[$ pour un $\delta > 0$. Comme de plus $f = P$ sur $\left[0, \alpha - \frac{\delta}{2}\right[$, on en déduit $P = Q$ sur $\left]\alpha - \delta, \alpha - \frac{\delta}{2}\right[$ et donc que le polynôme $P - Q$ a une infinité de racines, *i.e.* $P - Q = 0$. Ainsi, $f = P$ sur $[0, \alpha + \delta[$, ce qui contredit la maximalité de α.

Remarque. On peut généraliser l'énoncé aux polynômes à plusieurs indéterminées, cf. seconde feuille sur les polynômes.

10 Deux équations polynomiales : $P\left(X^2\right) = P(X) P(X \pm 1)$

- *Trouver tous les polynômes à ceofficients complexes tels que*

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

- *Trouver tous les polynômes à ceofficients réels tels que*

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

Solution proposée.

• Vu que l'on a affaire à une relation mettant en jeu des produits, on va raisonner sur des zéros. Éliminons de suite les candidat constants $P = 0$ ou 1, et soit ξ une racine complexe de P. FAIRE UN DESSIN !!!

En faisant $X = \xi$, on voit que ξ^2 est aussi racine de P, d'où une infinité ξ^{2^n} de racines pour P. On a donc deux possibilités : ou bien $\xi = 0$, ou bien $|\xi| = 1$, les cas restants donnant l'injectivé de la suite ξ^{2^n} et une infinité de racines distinctes pour P, pauvre petit polynôme de degré fini...

En faisant $X = \xi - 1$, on obtient une nouvelle racine $(\xi - 1)^2$, qui doit vérifier d'après ce qui précède $(\xi - 1)^2 = 0$ ou $\left|(\xi - 1)^2\right| = 1$, ce qui donne $\xi = 0$ ou $\xi = 1$ ou $\xi = e^{\pm i\frac{\pi}{6}}$.

Les valeurs $e^{\pm i\frac{\pi}{6}}$ sont à exclure car leurs carrés $e^{\pm i\frac{\pi}{3}}$ doivent être des racines de P et donc appartenir à $\left\{0, 1, e^{i\frac{\pi}{6}}, e^{-i\frac{\pi}{6}}\right\}$.

Si 0 n'était pas racine, faire $X = -1$ donnerait $P(1) = P(-1)P(0) \neq 0$, ce qui exclurait la racine 1 ; P n'aurait alors pas de racines, donc serait constant, ce que l'on a exclu.

P est par conséquent de la forme $X^\alpha (X-1)^\beta$. En réinjectant dans l'équation de départ, on trouve

$$X^{2\alpha}(X+1)^\beta (X-1)^\beta \overset{?}{=} X^\alpha (X-1)^\beta (X+1)^\alpha X^\beta,$$

ce qui est équivalent à $\alpha = \beta$.

Finalement, seuls le polynôme nul et les puissances de $X(1-X)$ sont solutions.

• On supposera P de degré ≥ 1 vu que les seuls candidats constants sont $P = 0$ ou 1. Appelons Z l'ensemble des racines complexes de P. (on ne redira pas de faire un dessin, même si on le pense très fort...).

Comme précédemment, Z est stable par élévation au carré, donc $Z \subset \{0\} \cup \{x \in \mathbb{C} ; |x| = 1\}$, puis Z est stable par $\xi \mapsto (\xi+1)^2$, d'où $Z \subset \left\{-1, e^{i\frac{\pi}{3}}, e^{-i\frac{\pi}{3}}\right\}$.

Faire $X = 0$ donne $P(0) = P(0)P(-1)$, ce qui exclut la racine -1.

Comme de plus P est à coefficients réels, les racines $e^{\pm i\frac{\pi}{3}}$ n'apparaissent que sous la forme "réelle" X^2+X+1 et donc P est du type

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

Cherchons les $n \geq 1$ pour lesquels l'équation de départ est satisfaite :

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

Tous les n conviennent !

Les solutions sont donc le polynôme nul et les puissances de X^2+X+1.

11 Sommes de Newton et fonctions symétriques élémentaires

Soit $a_1, ..., a_n$ des scalaires. On cherche des relations reliant les fonctions symétriques élémentaires $\sigma_k = \sum_{1\leq i_1<...<i_k\leq n} a_{i_1}...a_{i_k}$ aux sommes de Newton $S_k = a_1^k + ... + a_n^k$. On notera P le polynôme $\prod_{i=1}^n (X - a_i) = \sum_{i=0}^n (-1)^i \sigma_i X^{n-i}$.

• *Si $p \geq n$, montrer que*

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - ... + (-1)^p \sigma_n S_{p-n} = 0.$$

• *Si $1 \leq p \leq n$, montrer que*

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - ... + (-1)^{n-1} \sigma_{p-1} S_1 + (-1)^n \sigma_p p = 0.$$

(on pourra remarquer que $P' = \sum \frac{P}{X-a_i}$).

Solution proposée.

• Pour un i fixé on a

$$a_i^p - \sigma_1 a_i^{p-1} + \sigma_2 a_i^{p-2} - ... + (-1)^p \sigma_n a_i^{p-n} = a_i^{p-n}\left(a_i^n - \sigma_1 a_i^{n-1} + ... + (-1)^p \sigma_n\right) = a_i^{p-n} P(a_i) = 0,$$

d'où le résultat en sommant sur i.

- Toujours à i fixé, une division euclidienne de P par $X-a_i$ donne (à la main)

$$\frac{P}{X-a_i} = X^{n-1} + (a_i - \sigma_1) X^{n-2} + \left(a_i^2 - a_i\sigma_1 + \sigma_2\right) X^{n-3} + ... + \left(a_i^{n-1} - a_i^{n-2}\sigma_1 + ... + (-1)^{n-1}\sigma_{n-1}\right),$$

d'où en sommant sur i

$$\sum_{i=1}^{n} \frac{P}{X-a_i} = X^{n-1} + (S_1 - n\sigma_1) X^{n-2} + (S_2 - S_1\sigma_1 + n\sigma_2) X^{n-3} + ... + \left(S_{n-1} - S_{n-2}\sigma_1 + ... + (-1)^{n-1} n\sigma_{n-1}\right).$$

Pour $1 \leq p \leq n$, on regarde le coefficient en X^{p-1} dans $\sum_{i=1}^{n} \frac{P}{X-a_i} = P'$:

$$\begin{aligned} S_p - S_{p-1}\sigma_1 + ... + (-1)^{p-1}\sigma_{p-1}S_1 + (-1)^p n\sigma_p &= (n-p)(-1)^p\sigma_p, \\ S_p - S_{p-1}\sigma_1 + ... + (-1)^{p-1}\sigma_{p-1}S_1 + (-1)^p p\sigma_p &= 0. \end{aligned}$$

Une autre solution consiste à introduire la série génératrice

$$\left(\sum_{p\geq 0} S_p X^p\right) X^n P\left(\frac{1}{X}\right) \text{ où } P = \prod_{i=1}^{n} (X-a_i) = X^n - \sigma_1 X^{n-1} + ... + (-1)^n \sigma_n,$$

à voir comme un polynôme de degré infini sur lequel toutes les manipulations usuelles sont autorisées. On a d'une part

$$\begin{aligned} \left(\sum_{p\geq 0} S_p X^p\right) X^n P\left(\frac{1}{X}\right) &= \left(\sum_{p\geq 0}\sum_{i=1}^{n} a_i^p X^p\right) \prod_{i=1}^{n} (1-a_iX) = \left(\sum_{i=1}^{n}\sum_{p\geq 0} (a_iX)^p\right) \prod_{i=1}^{n} (1-a_iX) \\ &= \sum_{i=1}^{n} \frac{1}{1-a_iX} \prod_{i=1}^{n} (1-a_iX) = \sum_{i=1}^{n} \prod_{j\neq i} (1-a_jX) = \sum_{i=1}^{n} X^{n-1} \prod_{j\neq i} \left(\frac{1}{X} - a_j\right) \\ &= X^{n-1} P'\left(\frac{1}{X}\right) = X^{n-1}\left(\frac{n}{X^{n-1}} - \sigma_1 \frac{n-1}{X^{n-2}} + ... + (-1)^{n-1}\sigma_{n-1}\right) \\ &= n - (n-1)\sigma_1 X + (n-2)\sigma_2 X^2 + ... + (-1)^{n-1}\sigma_{n-1}X^{n-1} \\ &= \sum_{p=0}^{n-1} (-1)^p (n-p)\sigma_p X^p, \end{aligned}$$

d'autre part (en développant bêtement)

$$\begin{aligned} \left(\sum_{p\geq 0} S_p X^p\right) X^n P\left(\frac{1}{X}\right) &= \left(S_0 + S_1X + S_2X^2 + ... + S_nX^n + ...\right)\left(1 - \sigma_1X + \sigma_2X^2 + ... + (-1)^n\sigma_nX^n\right) \\ &= \sum_{p=0}^{n-1} \left(S_p - \sigma_1 S_{p-1} + ... + (-1)^p \sigma_p S_0\right) X^p + \sum_{p\geq n} \left(S_p - \sigma_1 S_{p-1} + ... + (-1)^n \sigma_n S_{p-n}\right) X^p, \end{aligned}$$

d'où le résultat en identifiant les coefficients des deux séries formelles.

Nous proposons une troisième solution, basée cette fois sur le calcul brut de $\sigma_k S_{p-k}$ pour $k = 0, ..., p-1$:

$$\begin{aligned} \sigma_k S_{p-k} &= \sum_{i_1<...<i_k} a_{i_1}...a_{i_k} \sum_{i=1}^{n} a_i^{p-k} = \sum_{\substack{i_1<...<i_k \\ i_{k+1}=1,...,n}} a_{i_1}...a_{i_k} a_{i_{k+1}}^{p-k} \\ &= \sum_{\substack{i_1<...<i_k \\ i_{k+1}\neq i_1,...,i_k}} a_{i_1}...a_{i_k} a_{i_{k+1}}^{p-k} + \sum_{j=1}^{k} \sum_{\substack{i_1<...<i_k \\ i_{k+1}=i_j}} a_{i_1}...a_{i_{j-1}} a_{i_j}^{p-k} a_{i_{j+1}}...a_{i_k} \\ &= \sum_{\substack{i_1<...<i_k \\ i_{k+1}\neq i_1,...,i_k}} a_{i_1}...a_{i_k} a_{i_{k+1}}^{p-k} + \sum_{\substack{i'_1<...<i'_{k-1} \\ i'_k\neq i'_1,...,i'_{k-1}}} a_{i'_1}...a_{i'_{k-1}} a_{i'_k}^{p-k} \\ &= \Sigma_k + \Sigma_{k-1} \end{aligned}$$

où l'on a naturellement introduit les quantités

$$\Sigma_k = \sum_{\substack{i_1<...<i_k \\ i_{k+1}\neq i_1,...,i_k}} a_{i_1}...a_{i_k} a_{i_{k+1}}^{p-k}.$$

Il en résulte un télescopage magique :

$$\begin{aligned} & S_p - S_{p-1}\sigma_1 + ... + (-1)^{p-1}\sigma_{p-1}S_1 + (-1)^p p\sigma_p \\ = & (\Sigma_1+\Sigma_0) - (\Sigma_0+\Sigma_1) + (\Sigma_1+\Sigma_2) ... + (-1)^{p-1}(\Sigma_{p-2}+\Sigma_{p-1}) + (-1)^p \sigma_p p \\ = & (-1)^p (p\sigma_p - \Sigma_{p-1}). \end{aligned}$$

Il reste à calculer Σ_{p-1} selon la place du dernier indice i_p parmi les autres :

$$\begin{aligned} \Sigma_{p-1} &= \sum_{\substack{i_1<...<i_{p-1} \\ i_p\neq i_1,...,i_{p-1}}} a_{i_1}...a_{i_{p-1}} a_{i_p} \\ &= \sum_{\substack{i_1<...<i_{p-1} \\ i_p<i_1}} a_{i_1}...a_{i_p} + \sum_{j=1}^{p-2} \sum_{\substack{i_1<...<i_{p-1} \\ i_j<i_p<i_{j+1}}} a_{i_1}...a_{i_p} + \sum_{\substack{i_1<...<i_{p-1} \\ i_p<i_{p-1}}} a_{i_1}...a_{i_p} \\ &= \sigma_p + (p-2)\sigma_p + \sigma_p, \; \textit{CQFD.} \end{aligned}$$

Remarque. On prendra garde à ne pas écrire pour $1 \leq p < n$

$$S_p - \sigma_1 S_{p-1} + \sigma_2 S_{p-2} - ... + (-1)^{n-1}\sigma_{p-1}S_1 + (-1)^n \sigma_p S_0 = 0.$$

(on a remplacé p à la fin par S_0). Ceci est tentant pour harmoniser avec le cas $p \geq n$ mais complètement faux vu que

$$S_0 = \sum_{i=1}^n a_i^0 = \sum_{i=1}^n 1 = n \neq p.$$

12 Sur les opérateurs de dérivation et le caractère scindé

On se place dans $\mathbb{R}[X]$. On considère l'opérateur linéaire de dérivation

$$\delta : P \mapsto P'.$$

Si n est un entier naturel, on définit δ^n comme la n-ième itérée de δ (noter que $\delta^0 = \mathrm{Id}$). On définit également $\lambda\delta^p + \mu\delta^q$ comme l'application $A \mapsto \lambda A^{(p)} + \mu A^{(q)}$. Enfi, si $A = \sum_{i\geq 0} a_i X^i$ est un polynôme, on définit $A(\delta)$ comme

$$A(\delta) = \sum_{i\geq 0} a_i \delta^i.$$

Montrer que si P et Q sont scindés sur $\mathbb{R}$, alors il en est de même pour $P(\delta)(Q)$. (on pourra d'abord regarder le cas $\deg P = 1$).

En déduire que si P est scindé sur $\mathbb{R}$, alors $\sum_{i=0}^n \binom{n}{i} P^{(i)}$ l'est aussi.

Solution proposée.
On peut toujours prendre P et Q unitaires.
Suivons l'énoncé et traitons pour commencer le cas $\deg P = 1$: $P = X - a$. On a donc

$$P(\delta)(Q) = Q' - aQ.$$

Afin de bien compter toutes les racines, scindons

$$Q=\prod_{i=1}^{n}\left(X-\lambda_i\right)^{\alpha_i}$$

où $n\geq 1$, $\alpha_i\geq 1$ et $\sum_{i=1}^{n}\alpha_i=\deg Q$.

La forme $Q'-aQ$ nous donne envie de faire apparaître $\frac{Q'}{Q}=\sum\frac{\alpha_i}{X-\lambda_i}$, ce qui suppose de se placer en dehors des racines de Q. Soit donc x réel distinct des λ_i ; on a

$$Q'\left(x\right)-aQ\left(x\right)=Q\left(x\right)\left(\frac{Q'\left(x\right)}{Q\left(x\right)}-a\right)=Q\left(x\right)\left(\sum_{i=1}^{n}\frac{\alpha_i}{x-\lambda_i}-a\right).$$

Le terme $\sum_{i=1}^{n}\frac{\alpha_i}{x-\lambda_i}-a$, consitué de n hyperboles emboitées, s'annule au moins $n-1$ fois (faire un dessin) car il passe continûment de ∞ à $-\infty$ entre chaque λ_i (il faut invoquer le théorème des valeurs intermédiaires), ce qui fournit $n-1$ racines distinctes pour $Q'-aQ$, en dehors des λ_i.

D'autre part, en regardant les racines multiples de Q, on voit que $Q'-\lambda Q$ a déjà $\sum_{i=1}^{n}\left(\alpha_i-1\right)=\deg Q-n$ racines parmi les λ_i (comptées avec leur multiplicité).

On a donc au total $\deg Q-1$ racines pour $Q'-aQ$ qui est de degré $\leq\deg Q$, ce qui montre que $Q'-aQ$ est scindé.

Une autre idée pour le cas $\deg P=1$ consiste à penser en terme d'équations différentielles. En effet, chercher les zéros de $Q'-aQ$ fait penser à l'équation $Q'-aQ=0$, de solution générique $Q=e^{a\,\mathrm{Id}}$. Comparons le comportement de Q et de cette solution $e^{a\,\mathrm{Id}}$ en dérivant le quotient

$$\partial_x\left[Q\left(x\right)e^{-ax}\right]=e^{-ax}\left(Q'\left(x\right)-aQ\left(x\right)\right)\ ;$$

le polynôme $Q'-aQ$ s'annule donc en même temps que la dérivée de $f=Qe^{-a\,\mathrm{Id}}$. Or les zéros $\lambda_1<...<\lambda_n$ de Q fournissent autant de zéros pour f, d'où (d'après Rolle) $n-1$ zéros pour f', un dans chaque intervalle $]\lambda_i,\lambda_{i+1}[$. On finit comme dans la première méthode.

Pour conclure, remarquons tout d'abord que si A et B sont deux polynômes réels alors $AB\left(\delta\right)=A\left(\delta\right)\circ B\left(\delta\right)$: il suffit de développer mentalement le produit. En scindant $P=P_1P^*$ où $\deg P_1=1$, on obtient donc

$$P\left(\delta\right)\left(Q\right)=P_1P^*\left(\delta\right)\left(Q\right)=\left[P_1\left(\delta\right)\circ P^*\left(\delta\right)\right]\left(Q\right)=\underbrace{P_1\left(\delta\right)\quad\underbrace{\left(P^*\left(\delta\right)\left(Q\right)\right)}_{\text{scindé par récurrence}}}_{\text{scindé d'après le cas }\deg P=1}.$$

Concernant le corollaire, il suffit d'appliquer à un polynôme Q scindé dont les coefficients seraient les binomiaux $\binom{n}{i}$: on essaie rapidement $Q=\left(X+1\right)^n$.

13 Polynômes et polygones

Soit $n\geq 1$ un entier et $z_0,...,z_n$ des complexes deux à deux distincts. On suppose que, pour tout polynôme $P\in\mathbb{C}\left[X\right]$ de degré $<n$, on a

$$P\left(z_0\right)=\frac{1}{n}\sum_{i=1}^{n}P\left(z_i\right).$$

Montrer que $z_1,...,z_n$ forment un polygône régulier dont le centre est z_0.

Solution proposée.

On commence par le cas $z_0=0$.

Introduisons quelques notations, à savoir les sommes de Newton $S_k=\sum_{i=1}^{n}z_i^k$ et les fonctions symétriques élémentaires $\sigma_k=\sum_{1\leq i_1<...<i_k\leq n}z_{i_1}...z_{i_k}$, qui sont reliées par les relations

$$\forall p=1,...,n,\ S_p-\sigma_1S_{p-1}+...+\left(-1\right)^{p-1}\sigma_{p-1}S_1+\left(-1\right)^p\sigma_pp=0$$

(cf. exercice précédent).

L'idée est d'utiliser l'hypothèse aux polynômes $P = X^k$, d'en déduire des informations sur les S_k, puis sur les σ_k, d'utiliser ces informations pour calculer le polnyôme $\prod_{i=1}^n (X - z_i)$, et enfin d'évaluer ce dernier en les z_k pour montrer que $z_1^n = ... = z_n^n$.

On applique l'hypothèse au polynômes $P = X^k$ pour $k = 0, ..., n-1$, ce qui donne

$$S_k = 0 \text{ pour tout } 0 \leq k < n,$$

et en réinjectant dans les relations entre les S_k et les σ_k, on obtient

$$\begin{cases} \sigma_p = 0 \text{ pour } 1 \leq p < n \\ S_n + n\sigma_n = 0 \text{ pour } p = n \end{cases}.$$

On en déduit $\prod_{i=1}^n (X - z_i) = X^n - (-1)^n \frac{S_n}{n}$, de sorte que, en évaluant en z_k, l'on obtienne $z_k^n = (-1)^n \frac{S_n}{n}$, ce qui ne dépend pas de k, d'où

$$z_1^n = ... = z_n^n = a^n$$

pour un $a \in \mathbb{C}$.

Alors les z_k (deux à deux distincts) sont exactement les racines du polynôme $\left(\frac{X}{a}\right)^n - 1$, d'où

$$z_k = ae^{2\pi i \frac{k}{n}} \text{ pour tout } k, \textit{ CQFD.}$$

Pour montrer le cas général, on remarque que $z_1 - z_0, ..., z_n - z_0$ vérifient les hypothèses du premier cas (car tout polynôme P peut s'écrire $Q(X + z_0)$), d'où

$$z_k = z_0 + ae^{2\pi i \frac{k}{n}}.$$

14 Polynômes symétriques et fonctions symétriques élémentaires

On se place dans $K[X_1, ..., X_n]$. On dira qu'un polynôme P dans $K[X_1, ..., X_n]$ est *symétrique* si

$$\forall \sigma \in \mathfrak{S}_n, \; P\left(X_{\sigma(1)}, ..., X_{\sigma(n)}\right) = P.$$

Des exemples de tels polynômes sont les *sommes de Newton* $S_k = \sum_{i=1}^n X_i^k$ ou bien les *polynômes symétriques élémentaires* $\sigma_k = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k}$. On précisera si besoin le nombre de variables des σ_k par un exposant :

$$\sigma_k^{(n)} := \sigma_k(X_1, ..., X_n).$$

On se propose de montrer que tout polynôme symétrique est un polynôme en les σ_k.

Montrer en lemme que si X_n divise un polynôme symétrique de $K[X_1, ..., X_n]$, alors ce dernier est divisible par $X_1 ... X_n$.

Soit $P \in K[X_1, ..., X_n]$ symétrique. Montrer qu'il existe un polynôme $S \in K[Y_1, ..., Y_n]$ tel que

$$P(X_1, ..., X_n) = S(\sigma_1, ..., \sigma_n).$$

Solution proposée.

Montrons le lemme par récurrence sur n. Pour $n = 1$, il s'agit de montrer que 0 est racine de P ssi $X \mid P$, ce qui ne pose pas de problème. On considère à présent $n \geq 2$ et P symétrique divisible par X_n, que l'on écrit

$$P = \sum_{i \geq 0} P_i X_n^i$$

où les $P_i \in K[X_1, ..., X_{n-1}]$ sont symétriques. L'hypothèse $P(X_1, ..., X_{n-1}, 0) = 0$ implique la nullité du terme "constant" $P_0 = 0$. P étant de plus invariant sous la transposition $(n-1, n)$, on doit avoir $P(X_1, ..., X_{n-2}, 0, X_n) =$

0, d'où $P_i(X_1, ..., X_{n-2}, 0) = 0$ pour tout i. Par hypothèse de récurrence, le produit $X_1...X_{n-1}$ doit diviser tous les P_i, et comme P_0 est nul, on peut factoriser en plus un X_n dans l'expression de P, d'où le lemme.

On fait une récurrence sur le nombre de variables plus le degré total.
• Pour $n = 1$, $X = \sigma_1$, donc $P = P(X) = P(\sigma_1)$.
• Pour $\deg P = 0$, *i.e.* $P = a$ constant, on a $P(X_1, ..., X_n) = a = a(\sigma_1, ..., \sigma_n)$.
• Soit P à $n \geq 2$ variables et de degré ≥ 1. On considère le polynôme à $n-1$ variables

$$p(X_1, ..., X_{n-1}) = P(X_1, ..., X_{n-1}, 0)$$

symétrique (car P l'est), donc on peut récurrer :

$$\begin{aligned} p(X_1, ..., X_{n-1}) &= Q\left(\sigma_1^{(n-1)}(X_1, ..., X_{n-1}), ..., \sigma_{n-1}^{(n-1)}(X_1, ..., X_{n-1})\right) \\ &= Q\left(\sigma_1^{(n)}(X_1, ..., X_{n-1}, 0), ..., \sigma_{n-1}^{(n)}(X_1, ..., X_{n-1}, 0)\right). \end{aligned}$$

On en déduit que $P(X_1, ..., X_n) - Q\left(\sigma_1^{(n)}, ..., \sigma_{n-1}^{(n)}\right)$ s'annule en $X_n = 0$, donc en tous les X_i par symétrie, donc est divisible par $X_1...X_n = \sigma_n$ par le lemme, d'où

$$P(X_1, ..., X_n) - Q\left(\sigma_1^{(n)}, ..., \sigma_{n-1}^{(n)}\right) = \sigma_n P^*$$

où P^* est un polynôme à n variables symétrique de degré $< \deg P$, et on peut alors récurrer sur le degré de P^*.

Remarque. On pourrait également montrer l'unicité avec un peu plus de travail. En notant $K[X_1, ..., X_n]^{\mathfrak{S}_n}$ les polynômes invariants par action de $\mathfrak{S}_n$ (*i.e.* les polynômes symétriques), on peut reformuler le résultat en disant que l'on dispose de l'isomorphisme

$$\left\{ \begin{array}{ccc} K[X_1, ..., X_n] & \simeq & K[X_1, ..., X_n]^{\mathfrak{S}_n} \\ P & \longmapsto & P(\sigma_1, ..., \sigma_n) \end{array} \right. .$$