# TD 14

## Polynômes Irréductibles

20. (a) 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) 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) 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)

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

puis

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

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)

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

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

(f)

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

(g) 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) 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) 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) 3. 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 $\mathbb{R}$[X] :

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

21. (a) 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) 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.

25. 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 $\mathbb{R}$[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 $\mathbb{R}$[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 .

## Approfondissements

25. (a) 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) i. L'ensemble considéré est une partie de $\mathbb{N}$ non vide car $I \neq \{0\}$.

ii. Il existe par construction $P \in I$ de degré $r$. Si on note $a$ son coefficient dominant alors $U = \dfrac{1}{a} \times P \in I$ par propriété d'idéal et est unitaire de degré $r$.

iii. 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 $P = UQ \in U\mathbb{K}[X]$.

27. 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 UP + VQ = 1. En notant $d$ le ppcm des dénominateurs des coefficients de U et V écrits sous forme fractionnaire et en posant A = $d$U et B = $d$ V, on a AP + 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. (a) Exploitons les égalités $\mathrm{P}(a) = \mathrm{P}(b) = \mathrm{P}(c) = 0$ en effectuant la division euclidienne de $\mathrm{X}^4$ 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 $\sigma_1, \sigma_2$ et $\sigma_3$ 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) Il suffit de calculer les fonctions symétriques élémentaires en $a^2, b^2$ et $c^2$. Notons-les $\Sigma_1, \Sigma_2$ et $\Sigma_3$. 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. (a) On remarque que $(\mathrm{X} - 1)\mathrm{P}_n = \mathrm{X}^n - 1$ donc les racines de $\mathrm{P}_n$ 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) Calculons $\mathrm{P}_n(1)$ de deux façons. D'une part, $\mathrm{P}_n(1) = n$ en utilisant l'expression de $\mathrm{P}_n$ 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) Posons $\mathrm{Q}_n = \mathrm{X}^n - e^{2in\theta}$. Les racines de $\mathrm{Q}_n$ sont les $e^{2i\left(\frac{k\pi}{n}+\theta\right)}$ pour $0 \leq k \leq n-1$. On a donc la factorisation suivante de $\mathrm{Q}_n$ 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)

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

Mais, l'ensemble des $\omega^{l-k}$ 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 $\mathrm{C}_n$ :

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

29. 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 $\left(a^2+b^2\right)^n = (a^n+b^n)^2$. 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 $\rho^{2n}$ 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. (a)

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

(b)

— 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 $(\mathrm{X}-\alpha)(\mathrm{X}-\bar{\alpha})=\mathrm{X}^2-2\,\mathrm{Re}(\alpha)\mathrm{X}+1$, où $\alpha$ est une racine $n$-ième de l'unité. Comme P est unitaire, il est produit de tels facteurs avec éventuellement $\mathrm{X}+1$ pour $n$ pair, de sorte que le terme constant de P est égal à 1 . On remarque d'autre part que si $\alpha$ 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 $\widehat{\mathrm{P}}=\mathrm{X}^{\deg(\mathrm{P})}\mathrm{P}\left(\frac{1}{\mathrm{X}}\right)$ 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 $k\in[\![0,p]\!]$, $a_{p-k}=a_k$. 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

$$a_k + b_k = a_k b_0 + a_0 b_k = 1 - \sum_{i=1}^{k-1} a_{k-i} b_i$$

"st, 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 $p+1 \leq k \leq q$ .