Corrigé X-ENS 2019, épreuve A, filière MP

Thème : *Polynômes cyclotomiques et nombres de Salem*

Partie I

1. L'application $P \mapsto P(\alpha)$ de $\mathbb{Q}[X]$ dans $\mathbb{C}$ est un morphisme d'anneaux. Son noyau $I(\alpha)$ est donc un idéal de $\mathbb{Q}[X]$. Il n'est pas réduit à $\{0\}$ puisque α est algébrique.

2. Si α est de degré 1, alors son polynôme minimal, qui est unitaire et annule α, est $X-\alpha$, donc $\alpha \in \mathbb{Q}$. Si, réciproquement, $\alpha \in \mathbb{Q}$, alors $X-\alpha \in \mathbb{Q}[X]$ donc $\Pi_\alpha = X-\alpha$ et α est de degré 1.

3. (a) Soient $A, B \in \mathbb{Q}[X]$ unitaires tels que $\Pi_\alpha = AB$. On a $A(\alpha)B(\alpha) = \Pi_\alpha(\alpha) = 0$ donc, par exemple, $A(\alpha) = 0$ d'où $A \in I(\alpha)$, c'est-à-dire $\Pi_\alpha | A$. On a donc $A = \Pi_\alpha$, ce qui montre que P est irréductible.

   (b) Puisque P annule z, z est algébrique et $\Pi_z | P$. Comme $\deg(\Pi_z) \geqslant 1$, que P est irréductible et que ces deux polynômes sont unitaires, $P = \Pi_z$.

   Remarque : une conséquence de ceci est que si w est une racine de Π_z, alors $\Pi_w = \Pi_z$.

4. (a) Soit α une racine commune de A et B. On a $\Pi_\alpha | A$ et $\Pi_\alpha | B$ donc, puisque $\deg(\Pi_\alpha) \geqslant 1$, A et B ne sont pas premiers entre eux.

   (b) D'une manière générale, les racines complexes d'un polynôme $P \in \mathbb{Q}[X]$ irréductible sont simples car $P \wedge P'$ divise P et $\deg(P \wedge P') < \deg(P)$, donc $P \wedge P' = 1$.

5. (a) Posons $\alpha = \dfrac{p}{q}$, où $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $p \wedge q = 1$. Soit $P = X^n + a_{n-1}X^{n-1} + \dots a_1 X + a_0 \in \mathbb{Q}[X]$ un polynôme annulateur de α. On a :

$$p^n + a_{n-1}p^{n-1}q + \dots a_1 p q^{n-1} + a_0 q^n = 0$$

   d'où $q | p^n$. Puisque $p \wedge q = 1$, et donc $p^n \wedge q = 1$, cela entraîne $q = 1$ et $\alpha \in \mathbb{Z}$.

   (b) Soit $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$. Comme $\Pi_\alpha | P$, les racines de Π_α sont des entiers algébriques. Or, Π_α étant unitaire, les relations coefficients-racines et le théorème admis en introduction montrent que les coefficients de Π_α sont des entiers algébriques. Comme ce sont des rationnels, la question **5.(a)** montre que ce sont des entiers : $\Pi_\alpha \in \mathbb{Z}[X]$.

6. (a) Soient $a, b \in \mathbb{Z}$ tels que $\alpha^2 + a\alpha + b = 0$. On a, en conjuguant, $\overline{\alpha}^2 + a\overline{\alpha} + b = 0$. Comme α n'est pas réel (car les réels de module 1 sont 1 et -1 qui ne sont pas algébriques de degré 2), α et $\overline{\alpha}$ sont les deux racines de $X^2 + aX + b$. Donc $b = \alpha\overline{\alpha} = 1$ et $a = \alpha + \overline{\alpha} = 2\,\mathrm{Re}(\alpha)$. En particulier, $|a| \leqslant 2$. Les cas $a = -2$ et $a = 2$ conduisent à $\alpha = \pm 1$ qui est exclu. Donc $a \in \{-1, 0, 1\}$ et $\alpha \in \{i, -i, j, -j, j^2, -j^2\}$, qui sont tous des complexes de module 1.

   (b) On a $\left|\dfrac{3+4i}{5}\right|^2 = \dfrac{9+16}{25} = 1$. Par ailleurs, le polynôme $\left(X - \dfrac{3+4i}{5}\right)\left(X - \dfrac{3-4i}{5}\right) = X^2 - \dfrac{6}{5}X + 1$ annule $\dfrac{3+4i}{5}$, qui est donc algébrique. Et, puisque $\dfrac{3+4i}{5}$ n'est pas rationnel, $\Pi_\alpha = X^2 - \dfrac{6}{5}X + 1$. Comme ce polynôme n'est pas à coefficients entiers, **5b.** montre que α n'est pas un entier algébrique. En particulier, ce n'est pas une racine de l'unité.

7. Notons $\mathbb{U}$ le groupe des complexes de module 1 et $\mathbb{U}_n$ le sous-groupe des racines n-ièmes de l'unité. L'ensemble $\mathbb{P}_n$ n'est autre que l'ensemble des générateurs de ce groupe. Notons $s(\omega)$ l'ordre d'une racine de l'unité, c'est-à-dire l'ordre du sous-groupe de $\mathbb{U}$ qu'elle engendre. On sait que :
— Si $d|n$, alors $\mathbb{U}_d \subset \mathbb{U}_n$
— si $\omega \in \mathbb{U}_n$, alors $s(\omega)$ divise n.
Donc $\{\omega \in \mathbb{U}_n ; s(\omega) = d\} = \mathbb{P}_d$ et

$$\mathbb{U}_n = \bigcup_{d|n} \{\omega \in \mathbb{U}_n ; s(\omega) = d\} = \bigcup_{d|n} \mathbb{P}_d$$

et cette réunion est disjointe. On en déduit immédiatement :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

8. (a) Soit $k \geqslant 1$. Les diviseurs de p^k sont les p^j, $1 \leqslant j \leqslant k$. Donc

$$\begin{cases} X^{p^k} - 1 = \prod_{j=1}^{k} \Phi_{p^j} \\ X^{p^{k-1}} - 1 = \prod_{j=1}^{k-1} \Phi_{p^j} \end{cases}$$

D'où :

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{p^{k-1} - 1} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \ldots + X^{p^{k-1}} + 1$$

(b) On trouve aisément : $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, et $\Phi_6 = X^2 - X + 1$.

9. (a) On a $\Phi_1 = X - 1$ donc $\Phi_1(0) = -1$. Par ailleurs on déduit de **7.** que, pour tout $n \in \mathbb{N}^*$, $\prod_{d|n} \Phi_d(0) = -1$. On en déduit immédiatement, par récurrence forte sur $n \geqslant 1$, que :

$$\Phi_n(0) = 1 \text{ si } n \geqslant 2 \ , \quad \Phi_n(0) = 1 \text{ si } n = 1 \ .$$

(b) On a d'abord $\Phi_1(1) = 0$. Et, si n est de la forme p^k, p premier, $k \geqslant 1$, alors **8a.** montre que $\Phi_{p^k} = p$. Par ailleurs, si n est de la forme $p_1^{k_1} \ldots p_s^{k_s}$, où $s \geqslant 2$, les p_i sont des nombres premiers distincts et $k_i \geqslant 1$, on déduit de **7b.** après simplification par $X - 1 = \Phi_1$:

$$n = \prod_{d|n, d \neq 1} \Phi_d(1)$$

d'où, en utilisant $\Phi_{p_j^k}(1) = p_j$

$$1 = \prod_{d|n, \rho(d) \geqslant 2} \Phi(d)$$

où l'on note $\rho(d)$ le nombre de diviseurs premiers de n (avec la convention usuelle que le produit vaut 1 si aucun diviseur d de n ne vérifie $\rho(d) \geqslant 2$). On en déduit immédiatement par récurrence forte sur $n \geqslant 2$ que :

$$\Phi_n(1) = p \text{ si } n \text{ est de la forme } p^k, \quad \Phi_n(1) = 1 \text{ sinon}$$

10. On a $X^n - 1 = \Phi_n \prod_{d|n, d<n} \Phi_d$. Donc Φ_n est le quotient (dans $\mathbb{Q}[X]$) dans la division euclidienne de $X^n - 1$ par $\prod_{d|n, d<n} \Phi_d$. Or l'algorithme usuel de la division euclidienne atteste que le quotient d'un polynôme de $\mathbb{Z}[X]$ par un polynôme unitaire de $\mathbb{Z}[X]$ est encore un polynôme de $\mathbb{Z}[X]$. Une récurrence forte sur $d|n$ montre alors que $\Phi_n \in \mathbb{Z}[X]$.

11. (a) On a $|a_k| \leqslant n$ pour tout k, donc le rayon de convergence de la série entière $\sum_k a_k z^k$ est au moins 1. En particulier, elle converge pour tout z tel que $|z| < 1$.

(b) Rappelons d'abord que la dérivée logarithmique d'un polynôme non nul Q, définie par $D(Q) = \dfrac{Q'}{Q}$, a la propriété $D(Q_1Q_2) = D(Q_1) + D(Q_2)$. Donc $D(P) = \displaystyle\sum_{k=1}^{n} \frac{1}{X - z_k}$. On a maintenant (l'inversion des deux Σ vient de ce que chaque série $\displaystyle\sum_{k=0}^{\infty} z_j^k z^k$ est convergente et que la seconde somme est finie) :

$$\begin{aligned} f(z) &= \sum_{k=0}^{\infty}\sum_{j=1}^{n} z_j^k z^k = \sum_{j=1}^{n}\sum_{k=0}^{\infty} z_j^k z^k = \sum_{j=1}^{n} \frac{1}{1 - z_j z} \\ &= \sum_{j=1}^{n} \frac{1}{z} \frac{1}{\frac{1}{z} - z_j} = \frac{1}{z}\frac{P'(1/z)}{P(1/z)}, \end{aligned}$$

d'où la relation cherchée.

(c) On a, pour z dans le disque unité ouvert privé de 0, $z^n P(1/z) f(z) = z^{n-1} P'(1/z)$. Donc la fonction $z \mapsto z^n P(1/z) f(z)$, définie sur le disque unité ouvert, produit d'une fonction polynomiale par la somme d'une série entière, est somme d'une série entière, laquelle vaut $z^{n-1}P'(1/z)$ (y compris pour $z = 0$ par continuité de la somme d'une série entière) : elle est donc à coefficients entiers. Posons $P = X^n + b_1 X^{n-1} + \ldots + b_{n-1}X + b_n$. On a $X^n P(1/X) = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + 1$. Donc les coefficients de la série entière de somme $z^n P(1/z) f(z)$ valent :

$$\begin{cases} a_0 \in \mathbb{Z} \\ a_1 + a_0 b_1 \in \mathbb{Z} \\ a_2 + a_1 b_1 + a_0 b_2 \in \mathbb{Z} \\ \ldots \end{cases}$$

et une récurrence immédiate montre que les a_k sont entiers.

12. (a) On a, vu ce qui précède, $a_k \in [\![-n, n]\!]$ pour tout k et, par conséquent, $(a_k, a_k + 1, \ldots, a_{k+n}) \in [\![-n, n]\!]^{n+1}$. L'application $k \mapsto (a_k, a_k + 1, \ldots, a_{k+n})$ de $\mathbb{N}$ dans $[\![-n, n]\!]^{n+1}$ ne peut donc pas être injective et il existe k, ℓ tels que $0 \leqslant k < \ell$ et

$$(a_k, a_k + 1, \ldots, a_{k+n}) = (a_\ell, a_\ell + 1, \ldots, a_{\ell+n}).$$

(b) Par linéarité, il suffit de vérifier l'égalité lorsque F est un polynôme de la forme X^s. Or

$$\sum_{i=1}^{n} z_i^s (z_i^\ell - z_i^k) = \sum_{i=1}^{n} z_i^{s+\ell} - \sum_{i=1}^{n} z_i^{s+k} = a_{s+\ell} - a_{s+k} = 0$$

(c) Comme P est irréductible, $P \wedge P'$, qui est un diviseur strict de P, vaut 1. Donc les racines complexes de P sont distinctes (rappelons que le pgcd de deux polynômes à coefficients dans $\mathbb{Q}$ est le même, que l'on voit ces polynômes comme éléments de $\mathbb{Q}[X]$ ou de $\mathbb{C}[X]$). Les relations obtenues dans **12b.** pour $F = X^s$ donnent, en prenant $s \in [\![0, n-1]\!]$:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ z_1 & z_2 & \dots & z_n \\ \vdots & \vdots & \dots & \vdots \\ z_1^{n-1} & z_2^n & \dots & z_n^{n-1} \end{pmatrix} \begin{pmatrix} z_1^\ell - z_1^k \\ z_2^\ell - z_2^k \\ \vdots \\ z_n^\ell - z_n^k \end{pmatrix} = 0$$

Comme les z_i sont deux à deux distincts, la matrice de Vandermonde est inversible d'où, pour tout i, $z_i^\ell = z_i^k$. Notons qu'on aurait pu, depuis **12a**, faire courir i dans $[\![0, n-1]\!]$ plutôt que $[\![0, n]\!]$.

13. (a) Il est bien connu que, pour $k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est un multiple de p. Cette propriété, et la formule du binôme, montrent l'existence de H.

(b) Puisque $z \in \mathbb{U}_n$, z est un entier algébrique. Donc, par **5b.**, $\Pi_z \in \mathbb{Z}[X]$. Posons $\Pi_z = X^s + b_{s-1}X^{s-1} + \ldots + b_1 X + b_0$. On a, en utilisant **13a.** étendu à la somme d'un nombre quelconque de polynômes (récurrence immédiate), l'existence d'un polynôme $G \in \mathbb{Z}[X]$ tel que

$$\Pi_z(X)^p = X^{sp} + b_{s-1}^p X^{p(s-1)} + \ldots b_1^p X^p + b_0^p + pG(X)$$

Or, par le petit théorème de Fermat, $b_k^p \equiv b_k\ [p]$. Donc il existe $F \in \mathbb{Z}[X]$ tel que

$$\Pi_z(X)^p = \Pi_z(X^p) + pF(X)$$

(c) La dernière relation entraîne :

$$\Pi_z(z^p) = pF(z)$$

Et, puisque l'ensemble des entiers algébriques est un anneau, $\dfrac{\Pi_z(z^p)}{p} = F(z)$ est un entier algébrique.

14. (a) On a

$$\prod_{i=1}^n P'(z_i) = \prod_{i=1}^n \prod_{j \neq i} (z_i - z_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (z_i - z_j)^2,$$

et, par ailleurs

$$\prod_{i=1}^n P'(z_i) = \prod_{i=1}^n n z_i^{n-1} = n^n \left(\prod_{i=1}^n z_i \right)^{n-1} = \left((-1)^{(n+1)} \right)^{n-1} n^n = (-1)^{n^2-1} n^n = (-1)^{n-1} n^n.$$

On en déduit

$$\prod_{i<j} (z_i - z_j)^2 = (-1)^{\frac{n(n+1)}{2}+1} n^n$$

(b) Les racines de Π_z sont bien sûr des éléments de $\mathbb{U}_n$ et elles sont distinctes (**4b.**). Posons $I = \{i \in [\![1, n]\!] ; \Pi_z(z_i) = 0\}$. Supposons $\Pi_z(z^p) \neq 0$. Alors, puisque $z^p \in \mathbb{U}_n$, il existe $k \in [\![1, n]\!] \setminus I$ tel que $z^p = z_k$. Il vient $\Pi_z(z^p) = \prod_{i \in I} (z_k - z_i)$. Or ce produit peut être isolé dans le produit étudié dans la question précédente :

$$\prod_{i<j} (z_i - z_j)^2 = v \Pi_z(z^p)$$

où v, qui est un produit de termes de la forme $(z_j - z_i)$, tous entiers algébriques, est un entier algébrique (via le théorème admis). Il vient $n^n = u \Pi_z(z^p)$, où $u = (-1)^{\frac{n(n+1)}{2}+1} v$ est un entier algébrique. Comme l'ensemble des entiers algébriques est un anneau (théorème admis), $\dfrac{n^n}{p} = u \times \dfrac{\Pi_z(z^p)}{p}$ est un entier algébrique. Comme $\dfrac{n^n}{p}$ est un rationnel, **5a.** montre que c'est un entier, ce qui est absurde puisque p est un nombre premier qui ne divise pas n. On a prouvé $\Pi_z(z^p) = 0$.

(c) Soit w un élément de $\mathbb{P}_n$ qui est aussi racine de Π_z. On a $\Pi_z = \Pi_w$ d'après **3b.** donc, par **14b.** appliqué à w, $\Pi_z(w^p) = \Pi_w(w^p) = 0$. En outre, w^p est encore élément de $\mathbb{P}_n$ puisque, on le sait, l'ordre de w^p dans $\mathbb{U}_n$ vaut $\dfrac{n}{n \wedge p} = n$. On en déduit aisément que, pour tout $k \in \mathbb{N}^*$ premier avec n, $\Pi_z(z^k) = 0$. Comme $\mathbb{P}_n = \{z^k, k \wedge n = 1\}$, il vient $\Phi_n | \Pi_z$ d'où, puisque Π_z est irréductible et que ces deux polynômes sont unitaires, $\Phi_n = \Pi_z$.

15. (a) C'est un calcul immédiat.

(b) Puisque P est unitaire et réciproque, son coefficient constant vaut 1 et 0 n'est pas racine de P : $x \neq 0$. Soit s l'ordre de x en tant que racine de P. Posons $P = (X - x)^s Q$, où $Q(x) \neq 0$. On a $P = X^d P(1/X) = X^s \left(\dfrac{1}{X} - x\right)^s X^{d-s} Q(1/X) = (1 - xX)^s X^{d-s} Q(1/X)$. Comme $1/x$ n'est pas racine de $Q(1/X)$, $1/x$ est racine d'ordre s de P.

16. Comme $\Pi_x \in \mathbb{Q}[X]$, $\dfrac{1}{x} = \overline{x}$ est racine de Π_x. Puisque $x \notin \{-1, 1\}$, $1/x$ est distinct de x. C'est donc un conjugué de x. On a donc, par **3a.**, $\Pi_{1/x} = \Pi_x$. Or, en notant d le degré de Π_x, $X^d \Pi_x(1/X)$ est un polynôme de degré d qui annule $1/x$. Donc il existe $\lambda \in \mathbb{Q}^*$ tel que $X^d \Pi_x(1/X) = \lambda \Pi_{1/x} = \Pi_x$. Ceci montre que l'ensemble Z des racines de Π_x est stable par $z \mapsto z^{-1}$. Comme 1 et -1 ne sont pas racines de Π_x (car leur polynôme minimal vaut $X - 1$ et $X + 1$ respectivement, tandis que toute racine de Π_x a Π_x pour polynôme minimal), on a $\prod_{z \in Z} z = 1$. Les racines de Π_x étant simples, il vient que $\deg(\Pi_x)$ est pair et $\Pi_x(0) = 1$. Ceci montre que $X^d \Pi_x(1/X)$ est unitaire, donc $\lambda = 1$. Par conséquent, Π_x est réciproque.

17. (a) On a $\gamma \notin \{-1, 1\}$ car -1 et 1 sont algébrique de degré 1, tandis que γ est algébrique de degré 2 (car $\Pi_\gamma = \Pi_\alpha$). Par **16.**, $\Pi_\alpha = \Pi_\gamma$ est réciproque.

(b) Si γ était une racine de l'unité, donc une racine de $X^m - 1$ pour une certain m, on aurait $\Pi_\gamma | X^m - 1$. Donc α serait une racine de l'unité et, puisque $\alpha \in \mathbb{R}$, α appartiendrait à $\{-1, 1\}$. Donc γ n'est pas une racine de l'unité.

(c) Si β est une racine de Π_α de module différent de 1, alors β ou $1/\beta$ est de module strictement supérieur à 1. Comme Π_α est réciproque, ce sont deux racines de Π_α. Or, par définition de $\mathcal{S}$, α est l'unique racine de Π_α de module strictement supérieur à 1. Donc $\beta = \alpha$ ou $\beta = \dfrac{1}{\alpha}$. On en déduit que tous les conjugués de α autres que $1/\alpha$ sont de module 1.

18. Si $\alpha \in \mathcal{S}$ est de degré impair, alors Π_α, dont toutes les racines sont distinctes (**4b.**), admet un nombre impair de racines. Comme toutes les racines autres que α et $1/\alpha$ sont de module 1, Π_α admet 1 ou -1 pour racine, ce qui est absurde (le degré de Π_α est au moins 2). Donc α est de degré pair. Si ce degré valait 2, on aurait $C(\alpha) = \{1/\alpha\}$, ce qui contredit la définition de $\mathcal{S}$. Donc le degré de α est pair, au moins égal à 4.

19. Si P_n admet une racine $z \in \mathbb{Q}$, alors z est un entier algébrique rationnel, donc, par **5a.**, $z \in \mathbb{Z}$. La relation $z(-z^3 + (6+n)z^2 - (10+n)z + (6+n)) = 1$ montre que z est inversible dans $\mathbb{Z}$, donc $z = \pm 1$. Or $P_n(1) = -n \neq 0$ et $P_n(-1) = 24 + 3n \neq 0$, donc P_n n'admet aucune racine rationnelle. Par ailleurs, puisque $P_n(1) < 0$ et $\lim_{x \to +\infty} P_n(x) = +\infty$, le théorème des valeurs intermédiaires montre que P_n admet une racine dans $]1, +\infty[$.

20. Comme P_n est un polynôme réciproque, cela résulte de **15b.**

21. On a

$$\frac{1}{X^2}[X^4-(6+n)X^3+(10+n)X^2-(6+n)X+1]=\left(X+\frac{1}{X}\right)^2-(6+n)\left(X+\frac{1}{X}\right)+(8+n)$$

Donc s_n et t_n sont racines de $Y^2-(6+n)Y+(8+n)$. Si $s_n \neq t_n$, ce sont les deux racines et l'on a

$$s_n+t_n=6+n \text{ et } s_nt_n=(8+n).$$

Ce résultat subsiste si $s_n=t_n$ car on a, dans ce cas, $\gamma_n=\alpha_n$ ou $\gamma_n=\dfrac{1}{\alpha_n}$:

$$X^4-(6+n)X^3+(10+n)X^2-(6+n)X+1=(X-\alpha_n)^2\left(X-\frac{1}{\alpha_n}\right)^2=\left(X^2-\left(\alpha_n+\frac{1}{\alpha_n}\right)X+1\right)^2,$$

d'où

$$\frac{1}{X^2}[X^4-(6+n)X^3+(10+n)X^2-(6+n)X+1]=\left(\left(X+\frac{1}{X}\right)-\left(\alpha_n+\frac{1}{\alpha_n}\right)\right)^2$$

qui montre que $s_n=t_n$ est racine double de $Y^2-(6+n)Y+(8+n)$.

22. Puisque α_n est réel, il en est de même de $t_n=\alpha_n+\dfrac{1}{\alpha_n}$ et de $s_n=6+n-t_n$. En outre, le polynôme $Q(Y)=Y^2-(6+n)Y+(8+n)$ vérifie $Q(0)>0$ et $Q(2)=-n<0$. Donc Q admet une racine dans $]0,2[$. Il ne peut s'agir de $t_n=\alpha_n+\dfrac{1}{\alpha_n}$ car $x+\dfrac{1}{x}>2$ pour tout $x>1$. Donc $s_n\in]0,2[$.
Comme $x+\dfrac{1}{x}$ n'appartient jamais à $]0,2[$ lorsque x est réel, on en déduit $\gamma_n\notin\mathbb{R}$. En outre, γ_n et $\dfrac{1}{\gamma_n}$ sont les deux racines du polynôme $X^2-s_nX+1=0$. Comme les coefficients de celui-ci sont réels, $\dfrac{1}{\gamma_n}=\overline{\gamma_n}$, d'où $|\gamma_n|=1$.

23. (a) Les nombres s_n et t_n sont les racines de $Y^2-(6+n)Y-(8+n)$. Ce sont donc des entiers algébriques. S'ils sont rationnels (ils le sont soit tous les deux, soit ni l'un ni l'autre puisque $s_n+t_n=6+n$), ce sont des entiers relatifs d'après **5a.** d'où, puisque $s_n\in]0,2[$, $s_n=1$. C'est absurde puisque 1 n'est manifestement pas racine de $Y^2-(6+n)Y-(8+n)$.

(b) Supposons P_n non irréductible et posons $P_n=AB$, où $A,B\in\mathbb{Q}[X]$ sont unitaires. Si on avait, par exemple, $\deg(A)=1$, alors P_n admettrait une racine rationnelle et s_n ou t_n serait rationnel. On a donc $\deg(A)=\deg(B)=2$. Les racines de A sont toutes les deux réelles ou tous les deux non réelles. Donc, quitte à échanger les noms de A et B : $A=(X-\alpha_n)\left(X-\dfrac{1}{\alpha_n}\right)$ d'où $t_n=\alpha_n+\dfrac{1}{\alpha_n}\in\mathbb{Q}$, ce qui contredit **23a.**. Donc P_n est irréductible. Puisque $|\gamma_n|=|1/\gamma_n|=1$, on a montré $\alpha_n\in\mathcal{S}$.

(c) On a $\alpha_n^4-6\alpha_n^3+10\alpha_n^2-6\alpha_n+1=n\alpha_n\left(\alpha_n^2-\alpha_n+1\right)$. Comme $x(x^2-x+1)\geqslant 1$ pour tout $x\geqslant 1$ (la dérivée de x^2-x+1 est positive sur $[1,+\infty[$), on a $\alpha_n^4-6\alpha_n^3+10\alpha_n^2-6\alpha_n+1\geqslant n$ et donc $\lim\limits_{n\to+\infty}\alpha_n^4-6\alpha_n^3+10\alpha_n^2-6\alpha_n+1=+\infty$. Or, si $(\alpha_n)_n$, qui est positive, ne divergeait pas vers $+\infty$, elle admettrait une sous-suite bornée, et la sous-suite correspondante de $(\alpha_n^4-6\alpha_n^3+10\alpha_n^2-6\alpha_n+1)_n$ serait elle-même bornée. Donc $\lim\limits_{n\to+\infty}\alpha_n=+\infty$.

24. Soit α un élément de $\mathcal{T}$. Posons $\Pi_\alpha=X^4+aX^3+bX^2+aX+1$ (on sait que Π_α est un polynôme réciproque). Notons α, $\dfrac{1}{\alpha}$, γ, $\dfrac{1}{\gamma}$ ses racines (où γ est de module 1). Les relations coefficients

racines donnent :

$$\begin{cases} a = -\left(\alpha + \dfrac{1}{\alpha} + \gamma + \dfrac{1}{\gamma}\right) \\ b = 2 + \alpha\gamma + \dfrac{1}{\alpha\gamma} + \dfrac{\alpha}{\gamma} + \dfrac{\gamma}{\alpha} \end{cases}$$

d'où $|a| \leqslant |\alpha| + 3$ et $|b| \leqslant 2|\alpha| + 4$. Ceci montre que, pour tout $M > 1$, l'ensemble d'éléments de $\mathcal{T}$ dans $]1, M]$ est fini, puisque, si α est un tel nombre, $|a| \leqslant M + 3$ et $|b| \leqslant 2M + 4$. En particulier, en choisissant M tel que $]1, M]$ contienne un élément de $\mathcal{T}$ (c'est possible d'après ce qui précède), on voit que $\mathcal{T}$ possède un plus petit élément.

Déterminons celui-ci. Soit $P = X^4 + aX^3 + bX^2 + aX + 1$ un polynôme réciproque de degré 4. Cherchons à quelles conditions l'une de ses racines est élément de $\mathcal{T}$. D'après la **partie 3**, P doit admettre une racine $\alpha > 1$ et une racine γ de module 1 non réelle (car non racine de l'unité), les autres racines étant $\dfrac{1}{\alpha}$ et $\dfrac{1}{\gamma}$. Supposons que tel soit le cas et posons $t = \alpha + \dfrac{1}{\alpha}$, $s = \gamma + \dfrac{1}{\gamma}$. Alors s et t sont les racines du polynôme $Q(Y) = Y^2 + aY + (b-2)$ et l'on a $t > 2$ et $-2 < s < 2$. Si, réciproquement, le polynôme $Q(Y) = Y^2 + aY + (b-2)$ admet deux racines réelles s et t vérifiant $t > 2$ et $-2 < s < 2$, alors les racines de P sont les racines des polynômes $X^2 - tX + 1$ et $X^2 - sX + 1$, qu'on peut écrire α, $\dfrac{1}{\alpha}$ pour le premier et γ, $\dfrac{1}{\gamma}$ pour le second, avec $\alpha > 1$ et $|\gamma| = 1$, γ non réel. En outre, dans ces conditions, P est irréductible si et seulement si s et/ou t est/sont irrationnels (comme $s + t$ est rationnel, ils le sont simultanément).

En résumé, P définit un élément de $\mathcal{T}$ si et seulement si $Q(Y) = Y^2 + aY + (b-2)$ admet deux racines réelles irrationnelles s et t vérifiant $t > 2$ et $-2 < s < 2$.
Par le théorème des valeurs intermédiaires, que $Q(Y) = Y^2 + aY + (b-2)$ admette deux racines réelles s et t vérifiant $t > 2$ et $-2 < s < 2$ équivaut à $Q(-2) > 0$ et $Q(2) < 0$, soit

$$\begin{cases} 2a - b - 2 < 0 \\ 2a + b + 2 < 0 \end{cases}$$

Déterminons maintenant le couple (a, b) (on verra qu'il n'y en a qu'un) vérifiant les deux inégalités de ce système pour lequel α est minimal (sans exiger a priori $\alpha \in \mathcal{T}$). Ainsi qu'on le constatera, t est irrationnel pour ce couple de valeurs, pour lequel on a aura donc $\alpha = \min(\mathcal{T})$.
En sommant les inégalités, on a $a < 0$ (donc $a \leqslant -1$ puisque c'est un entier).
Par ailleurs, puisque $x \mapsto x + 1/x$ est strictement croissante sur $]1, +\infty[$, α est minimal lorsque t est maximal.
Or $t = \dfrac{-a + \sqrt{a^2 - 4(b-2)}}{2}$ et, pour a fixé, l'application $b \mapsto \dfrac{-a + \sqrt{a^2 - 4(b-2)}}{2}$ est décroissante.
Donc, à $a \leqslant -1$ fixé, la valeur maximale de $t(a, .)$ est obtenue pour la valeur maximale de b vérifiant les deux inégalités, soit $b = -2a - 3$, et elle vaut

$$\tau(a) = \frac{-a + \sqrt{a^2 + 8a + 20}}{2}$$

Or cette fonction de a est une fonction décroissante. Sa valeur maximale est donc obtenue pour $a = -1$. Ainsi, la valeur maximale de t est obtenue pour $a = -1$ et $b = -1$. Comme $t = \dfrac{1 + \sqrt{13}}{2}$ est irrationnel, ce couple fournit la valeur minimale de $\alpha \in \mathcal{T}$:

$$\alpha = \frac{\frac{1+\sqrt{13}}{2} + \sqrt{\left(\frac{1+\sqrt{13}}{2}\right)^2 - 4}}{2} \simeq 1,722084$$