X-ENS MP Épreuve A 2019

Corrigé (copie modèle)

par Clément de Seguins Pazzis *

Partie 1

1. La fonction $\varphi : P \in \mathbb{Q}[X] \mapsto P(\alpha) \in \mathbb{Q}$ est un morphisme d'anneaux car elle vérifie

$$\varphi(1_{\mathbb{Q}[X]}) = 1$$

et

$$\forall (P,Q) \in \mathbb{Q}[X]^2,\ \varphi(P+Q) = \varphi(P) + \varphi(Q) \quad \text{et} \quad \varphi(PQ) = \varphi(P)\varphi(Q).$$

L'ensemble $I(\alpha)$ étant le noyau de ce morphisme, c'est un idéal de $\mathbb{Q}[X]$. Comme α est algébrique, $I(\alpha)$ possède un élément non nul.

2. Si α est de degré 1 alors $\Pi_\alpha = X + \beta$ pour un $\beta \in \mathbb{Q}$, et donc on trouve $\alpha + \beta = 0$ puis $\alpha = -\beta \in \mathbb{Q}$. Réciproquement, supposons $\alpha \in \mathbb{Q}$. Alors $X - \alpha \in I(\alpha)$, donc Π_α divise $X - \alpha$. Or Π_α ne peut être constant et non nul puisqu'il a une racine. Ainsi, Π_α est de degré 1, autrement dit α est de degré 1.

Ainsi, $\boxed{\alpha \text{ est de degré 1 si et seulement si } \alpha \in \mathbb{Q}.}$

3. **(a)** D'abord, on a vu dans notre réponse à la question **2** que Π_α n'est pas constant.

Ensuite, soit P, Q dans $\mathbb{Q}[X]$ tels que $\Pi_\alpha = PQ$. En particulier $\boxed{\deg P + \deg Q = \deg \Pi_\alpha}$ (et P et Q sont non nuls).

On a $P(\alpha)Q(\alpha) = \Pi_\alpha(\alpha) = 0$, donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$. Ainsi, Π_α divise P ou Q, ce qui conduit à $\deg \Pi_\alpha \leqslant \deg P$ ou $\deg \Pi_\alpha \leqslant \deg Q$. Par suite, $\deg Q \leqslant 0$ ou $\deg P \leqslant 0$, autrement dit Q ou P est constant.

Ainsi, $\boxed{\Pi_\alpha \text{ est irréductible dans } \mathbb{Q}[X].}$

(b) On suppose que $P(z) = 0$. Alors z est algébrique (puisque $P \neq 0$ et $P \in \mathbb{Q}[X]$), donc Π_z divise P. La question précédente montre que Π_z est irréductible, et comme P est aussi irréductible on en déduit que Π_z est associé à P. Puisque Π_z et P sont tous deux unitaires, on conclut que $\boxed{\Pi_z = P.}$

Remarque : en vu de la suite du sujet, il est important de remarquer qu'étant donné un nombre algébrique α, toute racine z de Π_α vérifie $\Pi_z = \Pi_\alpha$, ce que l'on déduit de **3.(a)** et **3.(b)**.

4. **(a)** Choisissons une racine commune $z \in \mathbb{C}$ de A et B. Supposons A et B premiers entre eux dans $\mathbb{Q}[X]$. Le théorème de Bézout fournit alors un couple $(U,V) \in \mathbb{Q}[X]^2$ tel que $AU + BV = 1$. En spécialisant en z, il vient $1 = A(z)U(z) + B(z)V(z) = 0$, ce qui est absurde. Ainsi, $\boxed{A \text{ et } B \text{ ne sont pas premiers entre eux dans } \mathbb{Q}[X].}$

Lycée Sainte-Geneviève, MP, dsp.prof@gmail.com

(b) On a vu en **3.(a)** que Π_α est irréductible, en particulier non constant. Par suite $\deg(\Pi'_\alpha) = \deg(\Pi_\alpha) - 1 \geqslant 0$, donc Π_α ne divise pas Π'_α. Comme Π_α est irréductible, cela montre qu'il est premier avec Π'_α. La contraposée du résultat précédent garantit alors que Π_α et Π'_α n'ont pas de racine complexe commune. Ainsi, toutes les racines complexes de Π_α sont simples.

5. (a) Soit $\alpha \in \mathbb{Q}$, supposé entier algébrique.
Écrivons $\alpha = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$ tels que $p \wedge q = 1$. Puisque α est un entier algébrique, il existe un polynôme $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ unitaire à coefficients entiers tel que $P(\alpha) = 0$.
Par suite $q^n P(\alpha) = 0$, ce qui se récrit

$$p^n = -q \sum_{k=0}^{n-1} q^{n-1-k} p^k a_k.$$

En particulier q divise p^n. Or q est premier avec p donc avec p^n. Le lemme de Gauss assure donc que q divise 1, autrement dit $q = \pm 1$. Ainsi, $\alpha = \pm p$ est un entier relatif.

(b) Soit $\alpha \in \mathbb{C}$, supposé entier algébrique. Il existe $P \in \mathbb{Z}[X]$ unitaire (de degré noté n) tel que $P(\alpha) = 0$. Le polynôme Π_α divise P, donc toutes ses racines sont des racines de P, et elles sont donc toutes des entiers algébriques. Notons $z_1, \dots, z_n$ ces racines (comptées à mesure de leur ordre de multiplicité).
Soit $k \in [\![1, n]\!]$. Alors, par les relations coefficients-racines, le coefficient de Π_α devant X^{n-k} vaut

$$a_k := (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} z_{i_1} \cdots z_{i_k}.$$

Comme l'ensemble des entiers algébriques est stable par addition, multiplication et passage à l'opposé (d'après le théorème admis), on en déduit que a_k est un entier algébrique. Or $a_k \in \mathbb{Q}$ (puisque $\Pi_\alpha \in \mathbb{Q}[X]$), et on déduit donc de **5.(a)** que $a_k \in \mathbb{Z}$.
Comme par ailleurs Π_α est unitaire, on conclut que $\Pi_\alpha \in \mathbb{Z}[X]$.

6. (a) Si $\alpha \in \mathbb{R}$, alors $\alpha = \pm 1$ donc α est racine 2-ième de l'unité.
Supposons α non réel. Alors $\overline{\alpha}$ est une autre racine complexe de Π_α (car Π_α est à coefficients réels) et ainsi, puisque α est de degré 2,

$$\Pi_\alpha = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2\operatorname{Re}(\alpha) X + 1.$$

Or Π_α est à coefficients entiers d'après **5.(b)**. Enfin $|2\operatorname{Re}(\alpha)| \leqslant 2|\alpha| = 2$, et ainsi Π_α est l'un des polynômes suivants : $X^2 - 2X + 1$, $X^2 - X + 1$, $X^2 + 1$, $X^2 + X + 1$ ou $X^2 + 2X + 1$, dont les ensembles de racines sont, respectivement, $\{1\}$, $\{-j, -\overline{j}\}$, $\{i, -i\}$, $\{j, \overline{j}\}$ et $\{-1\}$. Chacune de ces racines éventuelles est racine de l'unité, puisque $1^2 = (-1)^2$, $j^3 = (\overline{j})^3 = 1$, $(-j)^6 = (-\overline{j})^6 = 1$ et $i^4 = (-i)^4 = 1$. Ainsi, dans tous les cas α est une racine de l'unité.

(b) On a immédiatement $\left|\frac{3+4i}{5}\right| = \frac{\sqrt{3^2+4^2}}{5} = 1$. Les relations coefficients-racines montrent ensuite que

$$\left(X - \frac{3+4i}{5}\right)\left(X - \frac{3-4i}{5}\right) = X^2 - \frac{6}{5} X + 1.$$

Ce polynôme, noté Q, est donc à coefficients rationnels. Comme α en est une racine, on en déduit que α est algébrique et Π_α divise Q (donc α est de degré au plus 2). Évidemment α n'est pas rationnel (il n'est pas réel), donc la question **2** assure que α est de degré au moins 2. Ainsi, α est de degré 2. Enfin, Π_α divise Q et ces deux polynômes sont unitaires et de même degré, donc $\Pi_\alpha = Q$. En particulier $\Pi_\alpha \notin \mathbb{Z}[X]$, et on déduit de **5.(b)** que α n'est pas un entier algébrique.
Si α était une racine de l'unité il serait annulé par $X^n - 1$ pour un certain $n \in \mathbb{N}^*$ et serait donc un entier algébrique ! Ainsi, α n'est pas une racine de l'unité.

Partie 2

7. Notons $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. D'après le cours,

$$X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z).$$

Pour conclure, il suffit donc d'établir que la famille $(\mathbb{P}_d)_{d|n}$ partitionne $\mathbb{U}_n$.

Soit $d \in \mathbb{N}^*$ divisant n, alors $\mathbb{P}_d$ est l'ensemble des éléments d'ordre d du groupe $\mathbb{C}^*$ (ce que l'on reconnaît en utilisant une caractérisation classique de l'ordre). Or, étant donné $z \in \mathbb{C}$, l'égalité $z^n = 1$ équivaut au fait que z soit, dans $\mathbb{C}^*$, d'ordre fini divisant n. Cela montre que $\mathbb{U}_n = \bigcup_{d|n} \mathbb{P}_d$; en outre cette réunion est disjointe par unicité de l'ordre d'un élément dans un groupe. On conclut à l'identité

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

8. **(a)** Soit p un nombre premier et $k \geqslant 1$ un entier. En appliquant le résultat précédent aux entiers p^{k-1} et p^k, il reste

$$\frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \Phi_{p^k}$$

puisque, par primalité de p, les diviseurs de p^a (pour $a \in \mathbb{N}$) sont exactement les entiers de la forme p^b avec $b \in [\![0, a]\!]$. La formule dite de Bernoulli dans l'anneau commutatif $\mathbb{R}(X)$ assure donc que

$$\Phi_{p^k} = \frac{(X^{p^{k-1}})^p - 1}{X^{p^{k-1}} - 1} = \sum_{i=0}^{p-1} X^{ip^{k-1}}.$$

(b) Immédiatement $\Phi_1 = X - 1$ car $\mathbb{P}_1 = \{1\}$. En appliquant le résultat de **8.(a)**, on trouve aussi

$$\Phi_2 = X + 1,\ \Phi_3 = X^2 + X + 1,\ \Phi_4 = X^2 + 1 \quad \text{et} \quad \Phi_5 = X^4 + X^3 + X^2 + X + 1.$$

Enfin, dans $\mathbb{U}_6$ les éléments sont 1 (d'ordre 1), -1 (d'ordre 2), j et $\overline{j}$ (d'ordre 3) et $-j = e^{-\frac{i\pi}{3}}$ et $-j^2 = e^{\frac{i\pi}{3}}$ (d'ordre 6), donc

$$\Phi_6 = (X + j)(X + \overline{j}) = X^2 - X + 1.$$

9. **(a)** Montrons par récurrence forte que $\boxed{\Phi_k(0) = 1 \text{ pour tout } k \geqslant 2.}$ Notons que $\Phi_1(0) = -1$ vu le résultat de **8.(b)**.

Soit $k \geqslant 2$ tel que $\Phi_i(0) = 1$ pour tout $i \in [\![2, k-1]\!]$ (propriété trivialement vraie si $k = 2$). Alors, par **7**,

$$0^k - 1 = \prod_{d|k} \Phi_d(0) = \Phi_1(0)\Phi_k(0) \prod_{d|k,\ d \notin \{1,k\}} \Phi_d(1)$$

donc $-\Phi_k(0) = -1$ par l'hypothèse de récurrence, et finalement $\Phi_k(0) = 1$. Ainsi, l'hypothèse est vraie au rang suivant, ce qui achève le raisonnement par récurrence.

(b) Pour $k \geqslant 2$, on introduit la propriété

$$H_k : \ll\ \Phi_k(1) = 1 \text{ si } k \text{ possède plusieurs diviseurs premiers, sinon } \Phi_k(1) \text{ est l'unique diviseur premier de } k.\ \gg$$

Soit $k \geqslant 2$ tel que H_i soit vraie pour tout $i \in [\![2, k-1]\!]$ (à nouveau, cette condition est trivialement vraie lorsque $k = 2$). Supposons d'abord que $k = p^a$ pour un nombre premier p et un $a \in \mathbb{N}^*$. Alors, par **8.(a)**,

$$\Phi_k(1) = p.$$

Supposons maintenant que k possède plusieurs diviseurs premiers et notons B l'ensemble qu'ils forment. Par **7**,

$$\prod_{d|k,\ d>1} \Phi_d = \frac{X^n-1}{X-1} = \sum_{i=0}^{k-1} X^i$$

donc

$$\prod_{d|k,\ d>1} \Phi_d(1) = k$$

et ainsi

$$\Phi_k(1) = \frac{k}{\prod\limits_{d|k,1<d<k} \Phi_d(1)}.$$

Par l'hypothèse de récurrence, $\prod\limits_{d|k,1<d<k} \Phi_d(1) = \prod\limits_{d\in A} \Phi_d(1)$, où A désigne l'ensemble des diviseurs de k strictement supérieurs à 1 et qui sont puissances d'un nombre premier (ils sont tous distincts de k puisque l'on a supposé que k a plusieurs diviseurs premiers). Ce sont exactement les nombres de la forme p^a avec $p \in B$ et $a \in [\![1, \nu_p(k)]\!]$ (avec unicité d'une telle écriture) et ainsi, par l'hypothèse de récurrence,

$$\prod_{d|k,1<d<k} \Phi_d(1) = \prod_{p\in B} p^{\nu_p(k)} = k,$$

et on conclut que $\Phi_k(1) = 1$.

Ainsi, par récurrence forte $\boxed{H_k \text{ est validée pour tout } k \geqslant 2.}$

10. Procédons à nouveau par récurrence forte.

Soit $k \geqslant 2$. Supposons $\Phi_i \in \mathbb{Z}[X]$ pour tout $i \in [\![1, k-1]\!]$ (propriété clairement vraie si $k = 2$ puisque $\Phi_1 = X - 1$). Le polynôme $B := \prod\limits_{d|k,\ d<k} \Phi_d$ est donc à coefficients dans $\mathbb{Z}$ (l'énoncé admet que $(\mathbb{Z}[X], +, \times)$ est un anneau), et il est évidemment unitaire puisque produit de polynômes unitaires. Récrivons $B = \sum\limits_{i=0}^{e} a_i X^i$ pour une liste $(a_0, \dots, a_e)$ d'entiers, dont $a_e = 1$. Écrivons également $\Phi_k = \sum\limits_{i=0}^{+\infty} b_i X^i$. La relation $B\Phi_k = X^n - 1$ assure alors que

$$\forall l \geqslant e,\ \sum_{i=0}^{e} a_i b_{l-i} \in \mathbb{Z}.$$

Ainsi, pour tout $l \geqslant e$, il existe un entier c_l tel que

$$b_{l-e} = -\sum_{i=0}^{e-1} a_i b_{l-i} + c_l.$$

Or, tous les a_i sont entiers, et tous les b_i sont nuls à partir d'un certain rang. Par récurrence descendante forte, on en déduit que tous les b_i sont entiers (si, pour un $p \in \mathbb{N}$ donné, on a $b_i \in \mathbb{Z}$ pour tout entier $i > p$, on applique la formule précédente à $l := e + p$ et on en déduit que $b_p \in \mathbb{Z}$). Ainsi, $\Phi_k \in \mathbb{Z}[X]$.

On conclut par récurrence forte que $\boxed{\Phi_n \in \mathbb{Z}[X].}$

11. *Par souci de commodité nous fusionnons les réponses aux deux premières questions.*

(a) Soit $z \in \mathbb{C}$ tel que $|z| < 1$. Pour tout $i \in [\![1, n]\!]$, on a $|z_i z| = |z| < 1$, donc d'après le cours

$$\frac{1}{1 - z_i z} = \sum_{k=0}^{+\infty} (z_i z)^k.$$

Par addition de séries convergentes, on en déduit que $\sum_k a_k z^k$ converge et que

$$f(z) = \sum_{i=1}^{n} \frac{1}{1 - z_i z}.$$

Supposons maintenant z non nul. De $P = \prod_{i=1}^{n} (X - z_i)$, on déduit que $z^n P(z^{-1}) = \prod_{i=1}^{n} (1 - z_i z)$ donc

$$z^n f(z) P(z^{-1}) = \sum_{i=1}^{n} \prod_{j \neq i} (1 - z_j z).$$

Par ailleurs en dérivant P comme un produit (à $n-1$ reprises), on trouve

$$P' = \sum_{i=1}^{n} \prod_{j \neq i} (X - z_j)$$

donc de même

$$z^{n-1} P'(z^{-1}) = \sum_{i=1}^{n} \prod_{j \neq i} (1 - z_j z) = z^n f(z) P(z^{-1}). \tag{1}$$

Comme $z \neq 0$, on simplifie par z^{n-1} et on conclut que

$$\boxed{z f(z) P(z^{-1}) = P'(z^{-1}).}$$

(b) Voir **(a)**.

(c) On note $P = \sum_{k=0}^{n} b_{n-k} X^k$ avec $b_0 = 1$. On pose également $b_i := 0$ pour tout $i > n$. On trouve immédiatement, pour tout $z \in \mathbb{C}^*$,

$$z^n P(z^{-1}) = \sum_{k=0}^{n} b_k z^k = \sum_{k=0}^{+\infty} b_k z^k.$$

De même

$$z^{n-1} P'(z^{-1}) = \sum_{k=0}^{+\infty} b'_k z^k$$

où $b'_k = b_k(n-k)$ si $k < n$, et $b'_k = 0$ sinon. Par produit de Cauchy de séries entières sur l'intersection de leurs intervalles ouverts de convergence, on déduit de (1) que

$$\forall t \in]-1, 1[\setminus \{0\}, \quad \sum_{k=0}^{+\infty} b'_k t^k = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) t^k.$$

Cette relation est trivialement vraie pour $t = 0$ car $a_0 = n$, $b_0 = 1$ et $b'_0 = n$, donc par unicité du développement en série entière,

$$\forall k \in \mathbb{N}, \quad b'_k = \sum_{i=0}^{k} a_i b_{k-i}$$

ce qui se récrit

$$\forall k \geqslant 1, \quad a_k = -\sum_{i=0}^{k-1} a_i b_{k-i} + b'_k.$$

Comme tous les b_i et les b'_i sont entiers, et comme $a_0 = n$ (entier), on obtient par récurrence forte que $\boxed{a_k \text{ est entier pour tout } k \in \mathbb{N}.}$

12. **(a)** Nous remarquons que la suite $(a_k)_{k\geqslant 0}$ est bornée par n puisque

$$\forall k \in \mathbb{N},\ |a_k| \leqslant \sum_{i=1}^{n} |z_i^k| = n.$$

Comme les a_k sont tous entiers, ils sont dans $[\![-n, n]\!]$. La suite $(b_k)_{k\geqslant 0}$ définie par $b_k := (a_{k+i})_{0\leqslant i\leqslant n}$ prend donc ses valeurs dans l'ensemble $[\![-n, n]\!]^{n+1}$, lequel est fini en tant que produit cartésien (fini) d'ensembles finis. Cette suite n'est donc pas injective, autrement dit il existe deux entiers $0 \leqslant k < l$ tels que $b_k = b_l$, ce qui est la propriété souhaitée.

(b) Pour tout $p \in [\![0, n]\!]$, on a

$$\sum_{i=1}^{n} (z_i)^p (z_i^l - z_i^k) = a_{p+l} - a_{p+k} = 0,$$

donc par linéarité (évidente) de la fonction $F \in \mathbb{C}[X] \mapsto \sum_{i=1}^{n} F(z_i)(z_i^l - z_i^k)$, on en déduit

$$\boxed{\forall F \in \mathbb{C}_n[X],\ \sum_{i=1}^{n} F(z_i)(z_i^l - z_i^k) = 0.}$$

(c) Comme P est irréductible et unitaire dans $\mathbb{Q}[X]$, la question **3.(a)** montre que $P = \Pi_{z_1}$ et on déduit alors de **4.(b)** que les racines complexes de P sont toutes simples, autrement dit $z_1, \dots, z_n$ sont deux à deux distincts. Fixons $i \in [\![1, n]\!]$: on peut donc introduire Λ_i, le i-ème polynôme interpolateur élémentaire associé à la famille $(z_1, \dots, z_n)$, qui est de degré $n-1$. La relation de **12.(b)** appliquée à $F = \Lambda_i$ donne alors $z_i^l - z_i^k = 0$, autrement dit $z_i^{l-k} = 1$ puisque $z_i \neq 0$.
Comme $l - k \in \mathbb{N}^*$, on a effectivement montré que $\boxed{\text{tous les } z_i \text{ sont des racines de l'unité.}}$

13. **(a)** L'anneau $\mathbb{Z}[X]$ étant commutatif, la formule du binôme de Newton donne

$$(F+G)^p = \sum_{k=0}^{p} \binom{p}{k} F^{p-k} G^k = F^p + G^p + \sum_{k=1}^{p-1} \binom{p}{k} F^{p-k} G^k.$$

Fixons $k \in [\![1, p-1]\!]$ et notons que p divise $\binom{p}{k}$: en effet, comme p est premier il est premier avec tout élément de $[\![1, p-1]\!]$, donc avec $k!$. Comme $\binom{p}{k}$ est entier, on sait que $k!$ divise $p(p-1)\cdots(p-k+1)$, donc il divise $(p-1)\cdots(p-k+1)$ (Gauss), ce qui permet d'écrire $\binom{p}{k} = pc_k$ pour un entier c_k. Ainsi,

$$\sum_{k=1}^{p-1} \binom{p}{k} F^{p-k} G^k = p \underbrace{\sum_{k=1}^{p-1} c_k F^{p-k} G^k}_{H}.$$

Enfin, comme F et G sont dans $\mathbb{Z}[X]$ et comme $(\mathbb{Z}[X], +, \times)$ est un anneau, on conclut que $H \in \mathbb{Z}[X]$. Finalement

$$\boxed{(F+G)^p = F^p + G^p + pH \quad \text{où } H \in \mathbb{Z}[X].}$$

(b) Comme z est annulé par $X^n - 1$ c'est un entier algébrique. On sait donc par **5.(b)** que $\Pi_z \in \mathbb{Z}[X]$.
Ensuite, on généralise par récurrence le résultat de la question précédente : soit $k \in \mathbb{N}^*$. On définit la propriété

(H_k) : Pour tous $F_1, \dots, F_k$ dans $\mathbb{Z}[X]$, il existe un polynôme H tel que

$$(F_1 + \cdots + F_k)^p = \sum_{i=1}^{k} F_i^p + pH.$$

Ce résultat est en effet trivialement vrai pour $k = 1$ (prendre $H = 0$) et il a été établi au rang 2. Soit $k \geqslant 2$ tel que H_k soit vraie. Soit $F_1, \dots, F_{k+1}$ dans H_{k+1}. Posons $G := F_2 + \cdots + F_{k+1}$. Il existe $H_1 \in \mathbb{Z}[X]$ tel que $(F_1 + G)^p = (F_1)^p + G^p + pH_1$, et par l'hypothèse de récurrence il existe $H_2 \in \mathbb{Z}[X]$ tel que $G^p = \sum_{i=2}^{k+1} F_i^p + pH_2$. Ainsi,

$$(F_1 + \cdots + F_{k+1})^p = \sum_{i=1}^{k+1} (F_i)^p + p\underbrace{(H_1 + H_2)}_{\in \mathbb{Z}[X]}.$$

Ainsi, H_{k+1} est vraie. La propriété est donc établie à tout rang.

Écrivons en particulier $\Pi_z = \sum_{k=0}^{d} b_k X^k$. Les b_k sont entiers donc les $b_k X^k$ sont dans $\mathbb{Z}[X]$. Le résultat précédent fournit donc un $H \in \mathbb{Z}[X]$ tel que

$$(\Pi_z)^p = \sum_{k=0}^{d} (b_k X^k)^p + pH.$$

Enfin, pour tout $a \in \mathbb{Z}$, on sait que $a^p \equiv a\ [p]$ (petit théorème de Fermat) car $a^{p-1} \equiv 1\ [p]$ si p ne divise pas a (théorème d'Euler, car $p - 1 = \varphi(p)$ puisque p est premier), et sinon le résultat est trivial. Ainsi, le polynôme $G := \sum_{k=0}^{d} \frac{(b_k)^p - b_k}{p} X^{kp}$ est à coefficient entiers, et l'on a

$$\Pi_z(X^p) = (\Pi_z)^p + p\underbrace{(-G - H)}_{\in \mathbb{Z}[X]}.$$

(c) En spécialisant l'identité précédente en z, il vient $\Pi_z(z^p) = pF(z)$ donc

$$\frac{\Pi_z(z^p)}{p} = F(z).$$

Comme z est un entier algébrique le théorème admis montre que z^k l'est aussi pour tout $k \in \mathbb{N}$. Enfin, tout entier relatif i est évidemment un entier algébrique puisqu'annulé par $X - i$. Puisque $F \in \mathbb{Z}[X]$, le théorème admis montre alors que $F(z)$ est un entier algébrique, ce qu'il fallait démontrer.

14. (a) Avec la même formule de dérivation que celle utilisée en **11.(b)**, on voit que

$$\forall i \in [\![1, n]\!],\ P'(z_i) = \prod_{j \in [\![1,n]\!] \setminus \{i\}} (z_i - z_j).$$

Par ailleurs $P'(z_i) = n z_i^{n-1}$. En multipliant ces identités il vient donc

$$n^n \Big(\prod_{i=1}^{n} z_i\Big)^{n-1} = \prod_{i \neq j} (z_i - z_j).$$

Or, en regroupant les termes associés aux couples symétriques (i, j) et (j, i), on trouve

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

où N est le nombre de couples (i,j) d'entiers tels que $1 \leqslant i < j \leqslant n$, autrement dit $N = \binom{n}{2} = \frac{n(n-1)}{2}$. Enfin, les relations coefficients-racines montrent que $\prod_{i=1}^{n} z_i = (-1)^n P(0) = (-1)^{n-1}$, donc

$$\boxed{\prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2 = n^n (-1)^{(n-1)^2 - N} = n^n (-1)^{\frac{(n-1)(n-2)}{2}}.}$$

(b) On a déjà vu dans la démonstration de **6.(b)** que toute racine de l'unité est un entier algébrique. Comme $X^n - 1$ est à coefficients rationnels et annule z, il est divisible par Π_z, donc Π_z a toutes ses racines simples et parmi $z_1, \dots, z_n$. Notons B l'ensemble de ces racines. Par ailleurs $(z^p)^n = z^{np} = 1$ donc, quitte à réordonner les z_i (ce qui n'a aucune importance) on peut supposer $z^p = z_1$.
Raisonnons ensuite par l'absurde en suppoant que $\Pi_z(z^p) \neq 0$, autrement dit $z^p \notin B$. Quitte à réordonner à nouveau les z_i, on peut supposer que $B = \{z_2, \dots, z_q\}$ pour un certain entier $q \in [\![2, n]\!]$. Revenons au résultat intermédiaire

$$\prod_{i\neq j}(z_i - z_j) = \pm n^n$$

dans la question précédente. On peut alors factoriser

$$\prod_{i\neq j}(z_i - z_j) = \underbrace{\prod_{i=2}^{q}(z^p - z_i)}_{\Pi_z(z^p)} \underbrace{\prod_{i=q+1}^{n}(z_1 - z_i) \prod_{(i,j)\in C}(z_i - z_j)}_{u}$$

où C désigne l'ensemble des couples (i,j) d'éléments de $[\![1,n]\!]$ tels que $i \neq 1$ et $j \neq i$. Comme chaque élément z_i est un entier algébrique (car annulé par $X^n - 1$), le théorème admis montre que u en est aussi un. Finalement, $n^n = \pm u\,\Pi_z(z^p)$ pour un entier algébrique u.
Or par **13.(c)** on peut écrire $\Pi_z(z^p) = pv$ pour un entier algébrique v. Ainsi $n^n = \pm p(uv)$, et uv est un entier algébrique par le théorème admis. Par ailleurs $uv = \pm\frac{n^n}{p}$ est rationnel. La question **5.(a)** montre alors qu'il est entier, autrement dit p divise n^n. C'est absurde car p est premier et ne divise pas n.
On conclut que $\boxed{\Pi_z(z^p) = 0}$.

(c) Nous concluons d'abord la séquence précédente. La remarque faite à la fin de **3.(b)** montre que $\Pi_{z^p} = \Pi_z$. Remarquons ensuite que z^p reste dans $\mathbb{P}_n$: en effet, pour tout $k \in \mathbb{Z}$,

$$(z^p)^k = 1 \Leftrightarrow z^{pk} = 1 \Leftrightarrow n | pk \Leftrightarrow n | k$$

par le lemme de Gauss et les propriétés de l'ordre d'un élément (on a vu à la question **7** que les éléments de $\mathbb{P}_n$ sont les éléments d'ordre n dans le groupe $\mathbb{C}^*$). Ainsi, par récurrence finie (à partir de la décomposition en facteurs premiers de m), on trouve que pour tout entier naturel m premier avec n,

$$z^m \in \mathbb{P}_n \quad \text{et} \quad \Pi_{z^m} = \Pi_z.$$

Finalement, soit $y \in \mathbb{P}_n$. Comme z est d'ordre n dans le groupe $\mathbb{U}_n$ à n éléments, il engendre ce groupe et en particulier $y = z^k$ pour un $k \in \mathbb{N}$. Si k possédait un diviseur premier p commun avec n alors $y^{n/p} = z^{(k/p)n} = 1$ donc l'ordre de y ne serait pas n (mais un diviseur de n/p). Ainsi, k est premier avec n et le résultat précédent montre que $\Pi_y = \Pi_z$. En particulier y est racine de Π_z. Comme les racines de Φ_n sont simples, on conclut que

$$\Phi_n \mid \Pi_z.$$

Comme $\Phi_n \in \mathbb{Q}[X]$ et $\Phi_n(z) = 0$, on a inversement $\Pi_z \mid \Phi_n$, et finalement $\boxed{\Pi_z = \Phi_n}$ puisque Φ_n et Π_z sont unitaires.

Partie 3

15. **(a)** Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$ unitaire de degré d. Alors

$$X^d P(1/X) = X^d \sum_{k=0}^{d} a_k X^{-k} = \sum_{k=0}^{d} a_k X^{d-k} = \sum_{k=0}^{d} a_{d-k} X^k,$$

donc $X^d P(1/X) = P$ si et seulement si $\forall k \in [\![0, d]\!],\ a_k = a_{d-k}$, autrement dit si et seulement si P est un polynôme réciproque.

(b) Soit x une racine de P, de multiplicité notée p. Avec les notations précédentes, on a $P(0) = a_0 = a_d = 1$, donc $\boxed{x \neq 0.}$ On écrit ensuite

$$P = (X - x)^p Q(X)$$

où $Q \in \mathbb{C}[X]$ vérifie $Q(x) \neq 0$ et $\deg(Q) = n - p$. Alors

$$P = X^n P(1/X) = X^p (X^{-1} - x)^p X^{n-p} Q(X^{-1}) = (X - x^{-1})^p R(X)$$

où $R := (-x)^p X^{n-p} Q(X^{-1}) \in \mathbb{C}[X]$. En notant que $R(x^{-1}) = (-x)^p x^{p-n} Q(x) \neq 0$, on conclut que x^{-1} est d'ordre p comme racine de P, et en particulier $\boxed{x^{-1} \text{ est racine de } P.}$

16. Comme Π_x est à coefficients réels et x en est une racine, $\overline{x}$ en est aussi une racine, autrement dit $x^{-1} = \overline{x}$ en est une racine. Puisque $x \notin \{-1, 1\}$, on voit que $x^2 \neq 1$ donc $x \neq x^{-1}$ et ainsi $\boxed{x^{-1} \in \mathcal{C}(x).}$

La remarque à la fin de **3.(b)** assure que $\boxed{\Pi_{x^{-1}} = \Pi_x.}$

Notons d le degré de Π_x et constatons que $\Pi_{x^{-1}} = Q$ où $Q := X^d \Pi_x(X^{-1})$. D'abord, on voit que $Q(x^{-1}) = x^{-d}\Pi_x(x) = 0$, tandis que le calcul effectué en **15.(a)** montre que $Q \in \mathbb{Q}_d[X]$. On trouve donc que $\Pi_{x^{-1}}$ divise Q et en particulier x^{-1} est de degré au plus d. Comme x^{-1} est de module 1 et distinct de ± 1, le même raisonnement donne que le degré de x est au plus celui de x^{-1}, et finalement x^{-1} est de degré d. Ainsi la divisibilité de Q par $\Pi_{x^{-1}}$ et le fait qu'ils aient le même degré montre qu'ils sont associés. On a donc

$$\boxed{Q = \lambda \Pi_x \quad \text{pour un } \lambda \in \mathbb{C}^*.}$$

Par suite, Q et Π_x ont les mêmes racines. Or :

- Toute racine complexe de Π_x est non rationnelle puisque Π_x est irréductible et de degré au moins 2 (sinon x serait rationnel par **2**, donc égal à ± 1 car de module 1).
- En particulier, pour tout racine y de Π_x, on a $y \neq 0$ et y^{-1} est évidemment racine de Q.
- L'application $y \mapsto y^{-1}$ définit donc une involution sans point fixe de l'ensemble B des racines de Π_x dans lui-même. Enfin, les racines de Π_x sont toutes simples (voir **4.(b)**). En groupant chaque racine avec son inverse, on en déduit que $\boxed{\Pi_x \text{ est de degré pair}}$ et que le produit de ses racines complexes vaut 1, si bien que $\boxed{\Pi_x(0) = 1.}$

Finalement, $\Pi_x = \Pi_{x^{-1}} = \lambda X^d \Pi_x(X^{-1})$ pour un $\lambda \in \mathbb{C}^*$. En notant $a_0, \ldots, a_d$ les coefficients de Π_x, il vient alors

$$\forall k \in [\![0, d]\!],\ a_{d-k} = \lambda a_k.$$

Comme $a_d = 1$ (Π_x est unitaire) et $a_0 = \Pi_x(0) = 1$, on en déduit $\lambda = 1$ et ainsi $\boxed{\Pi_x \text{ est un polynôme réciproque.}}$

17. **(a)** Comme à la question précédente, on voit que $\boxed{\Pi_\alpha = \Pi_\gamma.}$ Si γ valait ± 1, le polynôme Π_α aurait une racine rationnelle bien qu'il soit irréductible de degré au moins 2, ce qui est absurde. Ainsi, la question **16** s'applique et montre que Π_γ est un polynôme réciproque. Comme α en est une racine (non nulle), la question **15.(b)** montre que α^{-1} en est aussi une, donc α^{-1} est racine de Π_α. Enfin, $\alpha \neq \alpha^{-1}$ puisque $\alpha \neq \pm 1$.

(b) Si γ était une racine de l'unité, Π_γ diviserait X^n-1 pour un $n\in\mathbb{N}^*$, et alors toutes les racines de Π_γ seraient de module 1. Ce n'est pas le cas puisque α en est une d'après le raisonnement effectué à la question précédente.

(c) Soit $\beta\in\mathcal{C}(\alpha)\setminus\{\alpha^{-1}\}$. En particulier $\beta\neq 0$ et β^{-1} est aussi racine de Π_α car Π_α est un polynôme réciproque. Comme $|\beta|\,|\beta^{-1}|=1$, si $|\beta|\neq 1$ alors $|\beta|>1$ ou $|\beta^{-1}|>1$, donc l'appartenance de α à $\mathcal{S}$ montrerait que $\beta=\alpha$ ou $\beta^{-1}=\alpha$, ce qui est interdit. Ainsi, $|\beta|=1$.
Tous les conjugués de α hormis α^{-1} sont donc de module 1.

18. Soit $\alpha\in\mathcal{S}$. Notons d le degré de Π_α. En particulier, l'existence d'un conjugué γ de α de module 1 est assurée, et on voit alors que $\Pi_\gamma=\Pi_\alpha$ par la remarque à la fin de **3.(b)**. On sait alors que Π_γ est un polynôme réciproque (voir **17.(a)**) dont ni 1 ni -1 n'est racine, et le raisonnement effectué en **16** a alors montré que Π_γ est de degré pair. Évidemment ce degré n'est pas 2 sinon α et α^{-1} (tous deux de module différent de 1 !) seraient les seules racines de Π_α. Ainsi,
α est de degré pair au moins égal à 4.

Partie 4

19. Soit $n>1$. Supposons que P_n ait une racine x dans $\mathbb{Q}$. D'après **5.(a)**, x est un entier. Par suite, l'égalité

$$x\big(-x^3+(6+n)x^2-(10+n)x+(6+n)\big)=1$$

montre que x est inversible dans l'anneau $\mathbb{Z}$, autrement dit $x=\pm 1$. Or, on calcule

$$P_n(1)=-n<0\quad\text{et}\quad P_n(-1)=3n+24>0,$$

ce qui donne une contradiction. Ainsi, P_n n'a pas de racine rationnelle. Par ailleurs, comme $x\mapsto P_n(x)$ est continue, le théorème des valeurs intermédiaires montre que $P_n([1,+\infty[)$ est un intervalle. Cet intervalle n'est pas majoré car évidemment $P_n\underset{+\infty}{\longrightarrow}+\infty$ (P_n est unitaire non constant) donc il inclut $[P_n(1),+\infty[$. Ainsi,
P_n a une racine dans $[1,+\infty[$, donc dans $]1,+\infty[$ puisque $P_n(1)<0$.

20. Par retour immédiat à la définition, P_n est un polynôme réciproque, donc le résultat annoncé se déduit directement de celui de **15.(b)**.

21. On remarque que s_n+t_n est la somme des racines de P_n (en tenant compte des ordres de multiplicités), donc par les relations coefficients-racines $-(s_n+t_n)$ est le coefficient de P_n devant X^3 (puisque P_n est unitaire de degré 4). Ainsi

$$\boxed{t_n+s_n=6+n.}$$

De même, en utilisant la deuxième fonction symétrique élémentaire, on trouve

$$\alpha_n\frac{1}{\alpha_n}+\alpha_n\gamma_n+\frac{\alpha_n}{\gamma_n}+\frac{1}{\alpha_n}\gamma_n+\frac{1}{\alpha_n}\frac{1}{\gamma_n}+\gamma_n\frac{1}{\gamma_n}=10+n,$$

soit

$$2+\alpha_n\gamma_n+\frac{\alpha_n}{\gamma_n}+\frac{\gamma_n}{\alpha_n}+\frac{1}{\alpha_n\gamma_n}=10+n,$$

et finalement, en retranchant 2 et en factorisant à gauche,

$$\boxed{t_ns_n=8+n.}$$

22. La question précédente, combinée aux relations coefficients-racines, montre que t_n et s_n sont les racines de

$$Q:=X^2-(6+n)X+(8+n).$$

Or,

$$Q(0) = 8 + n > 0 \quad \text{et} \quad Q(2) = -n < 0.$$

Puisque $t \mapsto Q(t)$ est continue, le théorème des valeurs intermédiaires montre que Q a au moins une racine dans $]0, 2[$. Or $t_n - 2 = \frac{(\alpha_n - 1)^2}{\alpha_n} \geqslant 0$. Nécessairement $0 < s_n < 2$. Si γ_n était réel, on trouverait que $|s_n| \geqslant 2$, car :

- si $\gamma_n > 0$ alors $s_n - 2 \geqslant 0$ (comme pour α_n) ;
- sinon, par le même raisonnement $(-s_n) - 2 \geqslant 0$.

On en déduit que $\boxed{\gamma_n \notin \mathbb{R}}$. Comme γ_n n'est pas réel, son conjugué ne l'est pas non plus mais c'est tout de même une racine de P_n (ce dernier étant à coefficients réels). Ainsi $\overline{\gamma_n} = \frac{1}{\gamma_n}$ (puisque $\overline{\gamma_n} \neq \gamma_n$), et on conclut que $|\gamma_n|^2 = 1$, autrement dit $\boxed{|\gamma_n| = 1.}$

23. **(a)** Les nombres t_n et s_n sont des entiers algébriques car racines du polynôme Q (unitaire à coefficients entiers) introduit précédemment. Supposons que l'un d'entre eux soit rationnel. La relation $t_n + s_n = 6 + n$ garantit alors que les deux sont rationnels, donc entiers d'après **5.(a)**. En particulier $s_n = 1$ puisque $0 < s_n < 2$. Il vient alors à la fois $t_n = 5 + n$ et $t_n = 8 + n$ en appliquant **21**, ce qui est contradictoire. Ainsi, $\boxed{s_n \text{ et } t_n \text{ sont tous deux irrationnels.}}$

(b) Par suite, ni α_n ni γ_n n'est rationnel, donc leurs inverses non plus. Ainsi, P_n n'a aucune racine rationnelle. Supposons-le réductible dans $\mathbb{Q}[X]$, en écrivant $P_n = AB$ avec A et B non constants à coefficients dans $\mathbb{Q}$, que l'on peut choisir unitaires quitte à les normaliser. Aucun des polynômes A et B ne peut être de degré 1 sinon P_n aurait une racine rationnelle, donc ils sont tous deux de degré 2. Quitte à les échanger, on peut supposer que α_n est racine de A. Mais alors les racines de A sont :

- ou bien α_n et α_n^{-1} ;
- ou bien α_n et γ_n ;
- ou bien α_n et γ_n^{-1} ;

et dans tous les cas leur somme n'est pas rationnelle puisque c'est t_n dans le premier cas, et un nombre non réel dans les deux autres cas. Or la somme des racines de A est l'opposé du coefficient de A selon X, donc un rationnel. Cette contradiction montre que $\boxed{P_n \text{ est irréductible dans } \mathbb{Q}[X].}$

Le nombre α_n est un entier algébrique puisqu'il est annulé par P_n (qui est unitaire et dans $\mathbb{Z}[X]$). Comme P_n est irréductible unitaire à coefficients rationnels, on sait par **3.(b)** que $\Pi_{\alpha_n} = P_n$. Les conjugués de α_n sont donc α_n^{-1}, γ_n et γ_n^{-1}. Les deux derniers sont de module 1 (voir **22**), tandis que $|\alpha_n^{-1}| = \frac{1}{\alpha_n} \leqslant 1$, donc $\boxed{\alpha_n \in \mathcal{S}.}$

(c) On note que $\forall n > 1,\ t_n = 6 + n - s_n \geqslant n + 4$, donc

$$t_n \underset{n \to +\infty}{\longrightarrow} +\infty.$$

Puis comme $\alpha_n = t_n - \frac{1}{a_n} \geqslant t_n - 1$ pour tout $n > 1$, on obtient par minoration que

$$\boxed{\alpha_n \underset{n \to +\infty}{\longrightarrow} +\infty.}$$

24. Commençons par un travail préliminaire en considérant un élément arbitraire α de $\mathcal{T}$. Son polynôme minimal est donc de degré 4 et réciproque, à coefficients entiers. Il s'écrit donc

$$P_{a,b} := X^4 - aX^3 + bX - aX + 1$$

pour un certain couple $(a, b) \in \mathbb{Z}^2$. Notons γ une racine de module 1 de ce polynôme et posons $t := \alpha + \alpha^{-1}$ et $s := \gamma + \gamma^{-1}$. Comme en **23.(a)**, on voit que t et s sont les racines du polynôme

$$Q_{a,b} := X^2 - aX + (b - 2)$$

et que $t > 2$ et $-2 < s < 2$. Pour cette dernière inégalité, remarquer que $s = 2\,\mathrm{Re}(\gamma)$ et que $-1 < \mathrm{Re}(\gamma) < 1$ car γ est de module 1 mais différent de ± 1 (sinon il serait de degré 1).

Réciproquement, donnons-nous un couple $(a,b)\in\mathbb{Z}^2$ tel que le polynôme $Q_{a,b}$ possède une racine réelle $t>2$ et une racine réelle $s\in\,]-2,2[$, avec t *irrationnel*. On montre facilement que X^2-tX+1 possède une unique racine réelle strictement supérieure à 1, notée α, et l'autre est α^{-1}, tandis que les racines de X^2-sX+1 sont non réelles et de module 1 : on en choisit une que l'on note γ, l'autre étant alors γ^{-1}. Alors,

$$P:=(X-\alpha)(X-\alpha^{-1})(X-\gamma)(X-\gamma^{-1})$$

vérifie

$$P=(X^2-tX+1)(X^2-sX+1)=X^4-(t+s)X^3+(2+ts)X^2-(t+s)X+1=P_{a,b.}$$

Il est à coefficients entiers, et on obtient alors que $\alpha\in\mathcal{S}$ sous réserve que P soit irréductible dans $\mathbb{Q}[X]$. Or P est nécessairement irréductible dans $\mathbb{Q}[X]$: en effet d'abord α est irrationnel puisque t l'est aussi ; puis s, qui vaut $a-t$, est aussi irrationnel ; on conclut alors comme à la question **23.(b)**.

Maintenant, considérons un couple $(a,b)\in\mathbb{Z}^2$ et voyons à quelle condition $Q:=X^2-aX+(b-2)$ possède une racine dans $]2,+\infty[$ et une racine dans $]-2,2[$ (condition notée $\mathcal{C}_{a,b}$). Il est bien sûr nécessaire que $Q(2)<0$. Si cette condition est réalisée, Q a une racine (unique) dans $]2,+\infty[$, et il a donc une racine dans $]-2,2[$ si et seulement si $Q(-2)>0$. Ainsi,

$$(\mathcal{C}_{a,b})\Leftrightarrow\begin{cases}Q(2)<0\\Q(-2)>0\end{cases}\Leftrightarrow\begin{cases}b<2a-2\\b>-2a-2\end{cases}\Leftrightarrow -2a-1\leqslant b\leqslant 2a-3.$$

Cette condition est réalisée en particulier pour le couple $(a,b)=(1,-1)$. Pour ce dernier $Q=X^2-X-3$ a sa plus grande racine t_0 irrationnelle (sinon d'après **5.(a)** t_0 serait un entier, mais on constate que $Q(2)<0$ et $Q(3)>0$, si bien que $2<t_0<3$). On notera que

$$t_0=\frac{1+\sqrt{13}}{2}.$$

Nous allons maintenant montrer que $t_0=\min\limits_{\alpha\in\mathcal{T}}(\alpha+\alpha^{-1})$. Pour cela, supposons par l'absurde qu'il existe $\alpha\in\mathcal{T}$ tel que $t:=\alpha+\alpha^{-1}$ soit strictement inférieur à t_0. Prenons $(a,b)\in\mathbb{Z}^2$ tel que $\Pi_\alpha=P_{a,b}$. Comme $2<t<t_0$ et la racine de $Q_{a,b}$ distincte de t doit être strictement inférieure à 2, on trouve $Q_{a,b}(t_0)>0$. Comme $t_0^2=t_0+3$, cela donne

$$(1-a)\,t_0+(b+1)>0,$$

autrement dit

$$(a-1)\,t_0\leqslant b+1.$$

Comme par ailleurs $b\leqslant 2a-3$, on en déduit $(a-1)t_0\leqslant 2a-2$ et donc

$$(a-1)(t_0-2)\leqslant 0.$$

Comme $t_0>2$ il vient $\boxed{a-1\leqslant 0.}$ Or $a=t_0+s$ pour un $s\in\,]-2,2[$, et donc $a>0$. Finalement $\boxed{a=1.}$ Enfin, l'encadrement $-2a-1\leqslant b\leqslant 2a-1$ donne $-3\leqslant b\leqslant -1$. La plus grande racine de $Q_{a,b}$ est donc $\frac{1+\sqrt{1-4(b-2)}}{2}$, supérieure ou égale à t_0 car $-4(b-2)\geqslant 4\times 3$. Cela contredit l'hypothèse initiale.

On conclut que $t_0=\min\limits_{\alpha\in\mathcal{T}}(\alpha+\alpha^{-1})$. Sur $]1,+\infty[$, la fonction $x\mapsto x+\frac{1}{x}$ est dérivable de dérivée $x\mapsto 1-\frac{1}{x^2}$ strictement positive, donc elle est strictement croissante. En notant α_0 la plus grande racine de $P_{1,-1}$, on conclut que

$$\boxed{\alpha_0=\min\mathcal{T}.}$$

Enfin, α_0 est évidemment la plus grande racine du polynôme X^2-t_0X+1, donc

$$\boxed{\alpha_0=\frac{t_0+\sqrt{t_0^2-4}}{2}\quad\text{avec}\quad t_0=\frac{1+\sqrt{13}}{2}}$$

(on s'abstiendra de simplifier l'expression de α_0).