

DM n° 21 : Polynômes, groupes symétriques

Corrigé du problème 1 – Simplicité de \mathfrak{A}_n

Préliminaire

1. Soit τ_1 et τ_2 deux transpositions.

- Si elles ont même support, alors $\tau_1 = \tau_2$ donc $\tau_1 \circ \tau_2 = \text{id}$, qui peut être vu par exemple comme la composée $(1\ 2\ 3) \circ (1\ 3\ 2)$.
- Si l'intersection de leur support est un singleton, il existe i, j et k deux à deux distincts tels que

$$\tau_1 = (i\ j) \quad \text{et} \quad \tau_2 = (i\ k).$$

Alors

$$\tau_1 \circ \tau_2 = (i\ j) \circ (i\ k) = (i\ k\ j).$$

- Si les supports de τ_1 et τ_2 sont disjoints, il existe i, j, k, ℓ deux à deux distincts tels que

$$\tau_1 = (i\ j) \quad \text{et} \quad \tau_2 = (k\ \ell).$$

On vérifie facilement que

$$(i\ j) \circ (k\ \ell) = (i\ j\ k) \circ (k\ \ell\ j).$$

Ainsi, toute composition de 2 transpositions est un 3-cycle ou une composée de deux 3-cycles.

2. Soit $\sigma \in \mathfrak{A}_n$. Il existe une décomposition de σ en un nombre pair de transpositions :

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2k}.$$

Chaque composée $\tau_{2i-1} \circ \tau_{2i}$, pour $i \in \llbracket 1, k \rrbracket$, s'écrit comme produit de 3-cycles, donc σ s'écrit également comme produit de 3-cycles.

Ainsi, les 3-cycles engendrent \mathfrak{A}_n .

Partie I – Conjugaison

On dit que deux permutations τ_1 et τ_2 de \mathfrak{S}_n sont conjuguées s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$.

1. • Soit $\sigma \in \mathfrak{S}_n$. On a alors $\text{id} \circ \sigma \circ \text{id}^{-1} = \sigma$, donc σ est conjuguée avec elle-même. La relation de conjugaison est donc réflexive.
- Soit τ_1 et τ_2 tels que τ_2 soit conjugué à τ_1 , c'est-à-dire qu'il existe σ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$. On a alors $\tau_1 = \sigma^{-1} \circ \tau_2 \circ \sigma$, donc τ_1 est conjugué de τ_2 (par $\sigma' = \sigma^{-1}$). Ainsi, la relation de conjugaison est symétrique.
- Soit τ_1, τ_2 et τ_3 tels que τ_1 et τ_2 sont conjugués ainsi que τ_2 et τ_3 . Il existe donc σ_1 et σ_2 tels que

$$\tau_2 = \sigma_1 \tau_1 \sigma_1^{-1} \quad \text{et} \quad \tau_3 = \sigma_2 \tau_2 \sigma_2^{-1} \quad \text{donc:} \quad \tau_3 = (\sigma_2 \sigma_1) \tau_1 (\sigma_2 \sigma_1)^{-1},$$

donc τ_3 est conjugué de τ_1 (par $\sigma_2 \sigma_1$). Ainsi la relation est transitive.

La relation de conjugaison est donc une relation d'équivalence.

2. Soit $\tau_1 = (i_1\ i_2\ \cdots\ i_k)$ un cycle, et $\tau_2 = \sigma \tau_1 \sigma^{-1}$.

- Soit $\ell \in \llbracket 1, k \rrbracket$. On a alors (en notant par convention $i_{k+1} = i_1$)

$$\tau_2(\sigma(i_\ell)) = \sigma \circ \tau_1 \circ \sigma^{-1} \circ \sigma(i_\ell) = \sigma \circ \tau_1(i_\ell) = \sigma(i_{\ell+1}).$$

Ainsi, $(\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$ est un cycle de τ_2 .

- Montrons qu'il s'agit du seul cycle non trivial. Soit pour cela $i \notin \{\sigma(i_1), \sigma(i_2), \dots, \sigma(i_k)\}$. On en déduit que $\sigma^{-1}(i) \notin \{i_1, i_2, \dots, i_k\}$, et donc $\sigma^{-1}(i)$ est un point fixe de τ_1 . Ainsi,

$$\tau_2(i) = \sigma\tau_1(\sigma^{-1}(i)) = \sigma(\sigma^{-1}(i)) = i.$$

Ainsi, i est un point fixe de σ .

- On en déduit que $(\sigma(i_1) \sigma(i_2) \dots \sigma(i_k))$ est le seul cycle non trivial de τ_2 , donc

$$\tau_2 = \sigma\tau_1\sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_k)).$$

3. • Soit τ_1 et τ_2 deux permutations, conjuguées par σ . Soit $\tau_1 = C_1 \circ \dots \circ C_s$ la décomposition en cycles à supports disjoints de τ_1 . On a alors :

$$\tau_2 = \sigma\tau_1\sigma^{-1} = (\sigma C_1 \sigma^{-1}) \circ (\sigma C_2 \sigma^{-1}) \circ \dots \circ (\sigma C_s \sigma^{-1}).$$

D'après la question précédente, les $\sigma C_i \sigma^{-1}$ sont des cycles de même longueur que C_i , et, σ étant bijective, l'expression trouvée dans la question précédente pour ces cycles montrent que leurs supports forment aussi une partition de $\llbracket 1, n \rrbracket$. Ainsi, il s'agit de la décomposition en cycles à supports disjoints de τ_2 . Les longueurs de ces cycles étant les mêmes que ceux de τ_1 , on en déduit que τ_1 et τ_2 ont même type cyclique.

- Réciproquement, soit τ_1 et τ_2 deux permutations de même type cyclique. Comme les produits de cycles à supports disjoints sont commutatifs, on peut alors trouver deux décompositions en cycles à supports disjoints (et formant une partition de $\llbracket 1, n \rrbracket$) :

$$\tau_1 = C_1 \circ \dots \circ C_k \quad \text{et} \quad \tau_2 = D_1 \circ \dots \circ D_k$$

tels que pour tout $i \in \llbracket 1, k \rrbracket$, les cycles C_i et D_i soient de même longueur. On peut donc trouver une suite $0 = \ell_1 < \ell_1 < \ell_2 < \dots < \ell_k = n$ et deux suites finies d'éléments de $\llbracket 1, n \rrbracket$: i_1, \dots, i_n et j_1, \dots, j_n tels que pour tout $\beta \in \llbracket 1, k \rrbracket$,

$$C_i = (i_{\ell_{i-1}+1} \dots i_{\ell_i}) \quad \text{et} \quad D_i = (j_{\ell_{i-1}+1} \dots j_{\ell_i}).$$

Comme par ailleurs, les supports des C_i forment une partition de $\llbracket 1, n \rrbracket$, la suite $(i_s)_{s \in \llbracket 1, n \rrbracket}$ représente en fait une permutation des éléments de $\llbracket 1, n \rrbracket$. De même pour $(j_s)_{s \in \llbracket 1, n \rrbracket}$. On définit alors de façon unique une permutation σ de $\llbracket 1, n \rrbracket$, en posant, pour tout $s \in \llbracket 1, n \rrbracket$, $\sigma(i_s) = j_s$. La description de la question précédente permet alors d'affirmer que pour tout $i \in \llbracket 1, k \rrbracket$,

$$D_i = \sigma C_i \sigma^{-1}, \quad \text{puis:} \quad \tau_2 = (\sigma C_1 \sigma^{-1}) \dots (\sigma C_k \sigma^{-1}) = \sigma \tau_1 \sigma^{-1}.$$

Ainsi, τ_1 et τ_2 sont conjugués.

Ainsi, deux permutations sont conjuguées dans \mathfrak{S}_n si et seulement si elles ont même type cyclique.

Partie II – Simplicité de \mathfrak{A}_5

1. On pose σ' dans \mathfrak{S}_n définie pour tout $i \in \llbracket 1, n \rrbracket$ par $\sigma'(a_i) = b_i$. Si σ' est pair, on pose $\sigma = \sigma'$ et sinon, $\sigma = \sigma' \circ (a_{n-1} a_n)$. Alors σ est paire et

$$\forall i \in \llbracket 1, n-2 \rrbracket, \quad \sigma(a_i) = b_i.$$

2. Soit $(a_1 a_2 a_3)$ et $(b_1 b_2 b_3)$ deux 3-cycle de \mathfrak{A}_5 . En appliquant la question précédente, il existe σ paire telle que $\sigma(a_1) = b_1$, $\sigma(a_2) = b_2$ et $\sigma(a_3) = b_3$. On a alors

$$\sigma(a_1 a_2 a_3) \sigma^{-1} = (\sigma(a_1) \sigma(a_2) \sigma(a_3)) = (b_1 b_2 b_3).$$

Ainsi, les cycles $(a_1 a_2 a_3)$ et $(b_1 b_2 b_3)$ sont conjugués dans \mathfrak{A}_5 (σ étant paire).

On en déduit que les 3-cycles sont 2 à 2 conjugués dans \mathfrak{A}_5 .

3. Soit $\sigma_1 = (i_1 j_1) \circ (k_1 \ell_1)$ et $\sigma_2 = (i_2 j_2) \circ (k_2 \ell_2)$ deux compositions de deux transpositions à supports disjoints. Les entiers i_1, j_1, k_1 et ℓ_1 sont donc deux à deux distincts dans $\llbracket 1, 5 \rrbracket$. Soit m_1 le dernier élément de $\llbracket 1, 5 \rrbracket$. On définit de même m_2 . Soit alors σ définie par $\sigma(i_s) = j_s$, pour tout $s \in \llbracket 1, 5 \rrbracket$. Quitte à considérer $\sigma \circ (i_1 j_1)$ au lieu de σ , on peut supposer σ est paire, et la description de la conjugaison sur les cycles amène :

$$\sigma \sigma_1 \sigma^{-1} = (\sigma(i_1) \sigma(j_1)) \circ (\sigma(k_1) \sigma(\ell_1)) = (i_2 j_2) \circ (k_2 \ell_2) = \sigma_2,$$

la composition éventuelle par $(i_1 j_1)$ n'ayant pas d'incidence (on trouve $(j_2 i_2)$ au lieu de $(i_2 j_2)$, mais c'est la même transposition!). Ainsi, σ étant paire, σ_1 et σ_2 sont conjuguées dans \mathfrak{A}_5 .

Ainsi les composées de deux transpositions à supports disjoints sont conjuguées dans \mathfrak{A}_5 .

4. Soit $c_0 = (1\ 2\ 3\ 4\ 5)$, et $c = (a_1\ a_2\ a_3\ a_4\ a_5)$ un 5-cycle, et $\sigma \in \mathfrak{S}_5$ définie par $\sigma(k) = a_k$. On a donc $c = \sigma c_0 \sigma^{-1}$. On en déduit que

$$c^2 = \sigma c_0 \sigma^{-1} \sigma c_0 \sigma^{-1} = \sigma c_0^2 \sigma^{-1} = \sigma(1\ 3\ 5\ 2\ 4) \sigma^{-1}.$$

Or,

$$(1\ 3\ 5\ 2\ 4) = \tau c_0 \tau^{-1},$$

où $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2\ 3\ 5\ 4)$.

On en déduit que $c^2 = (\sigma \circ \tau) \circ c_0 \circ (\sigma \circ \tau)^{-1}$.

5. La permutation τ ci-dessus est impaire (cycle de longueur 4). Ainsi, soit σ soit $\sigma \circ \tau$ est paire. On en déduit que soit c soit c^2 est conjugué dans \mathfrak{A}_5 à c_0 .
6. Soit H un sous-groupe distingué de \mathfrak{A}_5 . Puisque H est stable par conjugaison, et puisque les 3-cycles sont deux-à-deux conjugués, si H contient un 3-cycle, il les contient tous.

Le même argument montre que si H contient un produit de 2 transpositions disjointes, il les contient tous.

En ce qui concerne les 5-cycles, si H contient un 5-cycle c , il contient aussi c^2 . Ainsi, d'après la question précédente, par stabilité par conjugaison, il contient c_0 (notations de la question précédente). Or, étant donné un autre 5-cycle c' , soit c' soit c'^2 est conjugué à c_0 , donc c' est dans H ou c'^2 est dans H . Or, si $c'^2 \in H$, $c'^6 = c'^3 \in H$, et comme c' est d'ordre 5, $c' \in H$. Dans tous les cas, le 5-cycle c' , choisi quelconque, est dans H .

Ainsi, si H contient un 5-cycle, il les contient tous.

7. • Un 3-cycle est obtenu par le choix d'un sous-ensemble $\{i_1, i_2, i_3\}$ de $\llbracket 1, 5 \rrbracket$, puis le choix d'un des deux 3-cycles de support $\{i_1, i_2, i_3\}$, à savoir $(i_1\ i_2\ i_3)$ ou $(i_1\ i_3\ i_2)$. Il y a donc $\binom{3}{5} \times 2 = 20$ 3-cycles.
- Une composition de deux transpositions disjointes est la donnée d'un sous-ensemble $\{i_1\ i_2\ i_3\ i_4\}$ de $\llbracket 1, 5 \rrbracket$ (ou de façon équivalente, le choix du point fixe i_5), ce qui se fait de 5 façons possibles. Étant fixé arbitrairement un point par exemple i_1 de cet ensemble, on choisit son image (de 3 façons possibles), à savoir i_2 . Cela détermine toute la permutation, les deux derniers éléments s'échangeant l'un l'autre. Ainsi, il y a 15 compositions de 2 transpositions disjointes.
- Le choix d'un 5-cycle est obtenu en choisissant les u images successives de 1, d'abord parmi 4 éléments, puis pour la suivante parmi les 3 restants, etc. Il y a donc $4! = 24$ 5-cycles.
- Les seuls types cycliques possibles dans \mathfrak{A}_5 sont 1^5 (c'est l'identité), $1^2 3^1$, $1^1 2^2$ et 1^5 (car il faut un nombre impair de cycles dans la décomposition en produit de cycles à supports disjoints). Ainsi, si $H \neq \{\text{id}\}$, il contient au moins une permutation du type étudié précédemment, donc toutes les permutations de ce type (en plus de l'identité). Il ne peut pas contenir que des permutations d'un seul type (en plus de l'identité), sinon son cardinal serait 21, 16 ou 25, qui ne divise pas $|\mathfrak{A}_5| = 60$ (la moitié des permutations sont paires : la composition par une transposition fixée donne une bijection entre l'ensemble des permutations paires et l'ensemble des permutations impaires); cela contredit le théorème de Lagrange. H contient alors nécessairement, en plus de id , des permutations de deux types cycliques différents. Mais alors, un décompte rapide amène de façon immédiate $|H| > 30$. Comme $|H|$ doit diviser 60, il vient donc $|H| = 60$, donc $H = \mathfrak{A}_5$.
- Ainsi, les seuls groupes distingués de \mathfrak{A}_5 sont $\{0\}$ et \mathfrak{A}_5 . Autrement dit, \mathfrak{A}_5 est simple.

Partie III – Simplicité de \mathfrak{A}_n , $n > 5$

Soit $n > 5$, et soit H un sous-groupe distingué de \mathfrak{A}_n , différent de $\{\text{id}\}$. Soit $\sigma \neq \text{id}$ dans H

1. Soit a tel que $\sigma(a) \neq a$. On pose $b = \sigma(a)$, et on considère c différent de a, b et $\sigma(b)$. Soit τ le 3-cycle $(a b c)$.

La conjugaison préservant le type cyclique, $\sigma\tau^{-1}\sigma^{-1}$ est un 3-cycle.

Plus précisément, $\sigma\tau^{-1}\sigma^{-1} = (\sigma(a) \sigma(c) \sigma(b)) = (b \sigma(c) \sigma(b))$

Les entiers qui ne sont ni dans le support du cycle $\sigma\tau^{-1}\sigma^{-1}$ ni dans le support du cycle τ sont des points fixes de la composée $\tau\sigma\tau^{-1}\sigma^{-1}$. Or, l'union de ces deux supports est $\{a, b, c, \sigma(b), \sigma(c)\}$.

Ainsi, $\tau\sigma\tau^{-1}\sigma^{-1}$ admet au moins $n - 5$ points fixes.

2. Soit F un sous-ensemble de $\llbracket 1, n \rrbracket$ de cardinal 5, contenant l'ensemble des points non fixes de $\sigma\tau^{-1}\sigma^{-1}$. Soit $\mathfrak{A}(F)$ l'ensemble des permutations de \mathfrak{A}_n laissant tous les points extérieurs à F fixes. On a alors pour tout $\sigma \in \mathfrak{A}(F)$, $\sigma(F) = F$ (car σ est bijective). Donc σ induit une bijection $\tilde{\sigma}$ de F dans F

Soit $\varphi : \llbracket 1, 5 \rrbracket \longrightarrow F$ une bijection (numérotation des éléments de F). On définit alors :

$$\Phi : \mathfrak{A}(F) \longrightarrow \mathfrak{A}_5,$$

par $\Phi(\sigma) = \varphi^{-1} \circ \tilde{\sigma} \circ \varphi$.

• $\mathfrak{A}(F)$ est un sous-groupe de \mathfrak{A}_n . En effet :

* il contient id

* si σ et τ sont dans $\mathfrak{A}(F)$, alors tous les points hors de F sont points fixes de σ et τ , donc aussi de $\sigma \circ \tau$, et par conséquent, $\sigma \circ \tau \in \mathfrak{A}(F)$.

* Si $\sigma \in \mathfrak{A}(F)$, alors pour tout $x \notin F$, $\sigma(x) = x$, donc $\sigma^{-1}(x) = x$. Ainsi, l'ensemble des points non fixes de σ^{-1} est dans F , donc σ^{-1} est dans $\mathfrak{A}(F)$.

• Φ est un morphisme de groupes : en effet, soit σ et τ dans $\mathfrak{A}(F)$. Alors

$$\Phi(\sigma \circ \tau) = \varphi^{-1} \circ (\sigma \circ \tau) \circ \varphi = \varphi^{-1} \circ \sigma \varphi \circ \varphi^{-1} \circ \tau \circ \varphi = \Phi(\sigma) \circ \Phi(\tau).$$

• Φ est un isomorphisme, sa réciproque étant l'application qui à $\sigma \in \mathfrak{A}_5$ associé le prolongement (par l'identité) à $\llbracket 1, n \rrbracket$ de la bijection de F définie par $\varphi \circ \sigma \circ \varphi^{-1}$.

Ainsi, $\mathfrak{A}(F)$ est isomorphe, en tant que groupe, à \mathfrak{A}_5 .

Soit K un sous-groupe distingué de $\mathfrak{A}(F)$. On a alors pour tout $x \in \Phi(K)$ et tout $y \in \mathfrak{A}_5$, en posant $y' = \Phi^{-1}(y)$, et $x' = \Phi^{-1}(x)$,

$$yxy^{-1} = \Phi(y')\Phi(x')\Phi(y')^{-1} = \Phi(y'x'y'^{-1}).$$

Or, K étant distingué, et $x' \in H$, on a $y'x'y'^{-1} \in K$, donc $yxy^{-1} \in \Phi(K)$. On en déduit que $\Phi(K)$ est distingué dans \mathfrak{A}_5 , puis que $\Phi(K) = \{0\}$ ou \mathfrak{A}_5 , donc que $H = \{0\}$ ou $\mathfrak{A}(F)$.

Ainsi, $\mathfrak{A}(F)$ est simple.

3. Soit $K = H \cap \mathfrak{A}(F)$. Soit $x \in K$ et $y \in \mathfrak{A}(F)$. On a alors $xyx^{-1} \in \mathfrak{A}(F)$ (stabilité) et $xyx^{-1} \in H$ (car H est distingué dans \mathfrak{A}_n , et $x \in \mathfrak{A}_n$). Ainsi, $xyx^{-1} \in K$, d'où on tire que K est distingué dans $\mathfrak{A}(F)$.

Or, $\sigma \in H$, donc, H étant distingué, $\tau\sigma\tau^{-1} \in H$, et par stabilité par produit et inverse, $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Or $\tau\sigma\tau^{-1}\sigma^{-1} \in \mathfrak{A}(F)$, et cette permutation n'est pas l'identité. En effet, l'égalité

$$\tau\sigma\tau^{-1}\sigma^{-1} = (a b c) \circ (b \sigma(c) \sigma(b))$$

permet de se rendre compte que l'image de $\sigma(b)$ est c , qui est différent de $\sigma(b)$ par construction.

Ainsi, $K \neq \{\text{id}\}$. Étant distingué dans $\mathfrak{A}(F)$ qui est simple, on a donc $K = \mathfrak{A}(F)$, donc contient les 3-cycles de $\mathfrak{A}(F)$. Ainsi, H contient au moins un 3-cycle de \mathfrak{A}_n .

4. Les 3-cycles de \mathfrak{A}_n étant 2 à 2 conjugués, le fait que H soit distingué implique donc que tous les 3-cycles de \mathfrak{A}_n sont dans H . Puisque les 3-cycles engendrent \mathfrak{A}_n , il en résulte que $\mathfrak{A}_n \subset H$, l'autre inclusion provenant de la définition de H .

Ainsi, $H = \mathfrak{A}_n$.

Nous avons donc montré que tout sous-groupe distingué autre que $\{\text{id}\}$ de \mathfrak{A}_n est égal à \mathfrak{A}_n lui-même. Ceci équivaut à affirmer que \mathfrak{A}_n est simple (pour $n \geq 5$).

Corrigé du problème 2 – (Autour de la conjecture d'Ilieff-Sendov, d'après ENS 1989)

Questions préliminaires

1. D'après le théorème de d'Alembert-Gauss, P possède autant de racines (comptées avec multiplicité) que son degré, donc

$$\boxed{\sum_{i=0}^m n_i = n.}$$

2. Le polynôme P se factorise de la façon suivante (attention à ne pas oublier le coefficient dominant) :

$$\boxed{P = a_n \prod_{i=0}^m (X - z_i)^{n_i}.}$$

Partie I – Quelques cas simples de la conjecture

1. Cas des polynômes de degré 2

On suppose ici que $n = 2$.

- (a) On part de la forme factorisée de $P = a_2(X - s_1)(X - s_2)$, où s_1 et s_2 sont les deux racines de P , non nécessairement distinctes. On a alors :

$$P' = a_2(X - s_2) + a_2(X - s_1) = 2a_2 \left(X - \frac{s_1 + s_2}{2} \right).$$

Par conséquent, l'unique racine de P' est $\boxed{\zeta = \frac{s_1 + s_2}{2}}$.

- (b) On a alors

$$|s_1 - \zeta| = \left| s_1 - \frac{s_1 + s_2}{2} \right| = \left| \frac{s_1 - s_2}{2} \right| \leq \frac{|s_1| + |s_2|}{2},$$

et comme les racines de P sont supposées de module au plus 1, $|s_1 - \zeta| \leq 1$. Ainsi, P vérifie $\mathcal{IS}(s_1)$. La symétrie du rôle des deux racines nous assure que P vérifie aussi $\mathcal{IS}(s_2)$. Donc $\boxed{P \text{ vérifie } \mathcal{IS}}$.

2. Cas d'une racine multiple

Si $n_0 \geq 2$, z_0 est racine de multiplicité $n_0 - 1 > 0$ de P' . En posant $\zeta = z_0$, racine de P' , on a bien $|z_0 - \zeta| = 0 \leq 1$, donc $\boxed{P \text{ vérifie } \mathcal{IS}(z_0)}$.

3. Cas d'un polynôme ayant peu de racines distinctes

- (a) Les z_i sont racines de multiplicité exactement $n_i - 1$ de P' (donc non racines de P si $n_i = 1$). Les autres racines de P' ne sont alors pas racines de P , et sont, d'après le théorème de d'Alembert-Gauss, en nombre égal à

$$(n - 1) - \sum_{i=0}^m (n_i - 1) = n - 1 + (m + 1) - \sum_{i=0}^m n_i = n - 1 + (m + 1) - n = m.$$

Notons w_1, \dots, w_m ces m racines, non nécessairement distinctes entre elles, mais différentes des z_i . Connaissant toutes les racines de P' , ainsi que son coefficient dominant (le monôme dominant est $na_n X^{n-1}$, obtenu en dérivant $a_n X^n$), on peut écrire la factorisation de P' en facteurs irréductibles : factorisation de P' s'écrit alors :

$$\boxed{P' = na_n \prod_{i=0}^m (X - z_i)^{n_i - 1} \prod_{j=1}^m (X - w_j).}$$

- (b) On suppose que $n_0 = 1$. Alors, le facteur $(X - z_0)^{n_0 - 1}$ est égal à 0. En évaluant l'expression précédente en z_0 , on obtient :

$$P'(z_0) = na_n \prod_{i=1}^m (z_0 - z_i)^{n_i - 1} \prod_{j=1}^m (z_0 - w_j).$$

Par ailleurs, en posant $Q = a_n \prod_{i=1}^m (X - z_i)^{n_i}$, on a

$$P = (X - z_0)Q, \quad \text{donc} \quad P' = (X - z_0)Q' + Q.$$

En évaluant en z_0 , il vient :

$$P'(z_0) = Q(z_0) = a_n \prod_{i=1}^m (z_0 - z_i)^{n_i}.$$

En comparant les deux expressions obtenues, et en simplifiant par $a_n \prod_{i=1}^m (z_0 - z_i)^{n_i-1} \neq 0$, il vient :

$$n \prod_{j=1}^m (z_0 - w_j) = \prod_{i=1}^m (z_0 - z_i).$$

Comme pour tout $i \in \llbracket 1, m \rrbracket$, $|z_i| \leq m$, on obtient, par inégalité triangulaire, $|z_0 - z_i| \leq |z_0| + |z_i| \leq 2$. Ainsi,

$$\left| \prod_{j=1}^m (z_0 - w_j) \right| \leq \frac{2^m}{n}.$$

Par conséquent, si $n \geq 2^m$,

$$\left| \prod_{j=1}^m (z_0 - w_j) \right| \leq 1.$$

Ce produit est non vide (P' ayant au moins une racine d'après d'Alembert-Gauss, étant de degré $n-1 \geq 1$).

Un raisonnement par l'absurde élémentaire montre qu'au moins un de ses facteurs vérifie $|z_0 - w_j| \leq 1$.

Ainsi, il existe une racine $w_j \in \text{Rac}(P')$ telle que $|z_0 - w_j| \leq 1$, donc $\boxed{P \text{ vérifie } \mathcal{IS}(z_0)}$.

- (c) Soit $n \geq 2^m$. Quitte à renuméroter les racines, toute racine simple de P peut jouer le rôle de z_0 dans l'argument précédent. Ainsi, pour toute racine simple z de P , P vérifie $\mathcal{IS}(z)$. D'après I-2, pour toute racine multiple z de P , P vérifie aussi $\mathcal{IS}(z)$. On en déduit bien que $\boxed{P \text{ vérifie } \mathcal{IS}}$.

Partie II – Étude du cas de certaines racines

1. Cas de la racine nulle

On suppose dans cette question que $z_0 = 0$.

- (a) D'après le cours,

$$\frac{P'}{P} = \sum_{i=0}^m \frac{n_i}{X - z_i}.$$

- (b) Soit $j \in \llbracket 1, m \rrbracket$. Puisque w_j est racine de P' mais pas de P , on a :

$$0 = \frac{P'}{P}(w_j) = \sum_{i=0}^m \frac{n_i}{w_j - z_i} = \sum_{i=0}^m n_i \frac{\overline{w_j - z_i}}{|w_j - z_i|^2}.$$

En conjuguant cette expression, et en passant la moitié de la somme de l'autre côté, il vient :

$$w_j \sum_{i=0}^m \frac{n_i}{|w_j - z_i|^2} = \sum_{i=0}^m \frac{n_i}{|w_j - z_i|^2} z_i.$$

En posant pour tout $i \in \llbracket 0, m \rrbracket$,

$$\lambda_i = \frac{n_i}{|w_j - z_i|^2} > 0, \quad \text{et} \quad \mu_i = \frac{\lambda_i}{\sum_{i=0}^m \lambda_i},$$

on a bien $\sum_{i=0}^m \mu_i = 1$, $\mu_i > 0$ et

$$w_j = \sum_{i=0}^m \mu_i z_i.$$

Ainsi, $\boxed{w_j \text{ est barycentre à coefficients strictements positifs des } z_i}$.

On a alors, d'après l'inégalité triangulaire :

$$|w_j| \leq \sum_{i=0}^m \mu_i |z_i| \leq \sum_{i=0}^m \mu_i = 1.$$

Donc $|w_j| \leq 1$.

- (c) Puisque P' est de degré au moins 1, il admet une racine w , qui est de module au plus 1 (soit w est déjà racine de P et on obtient cette inégalité par les hypothèses faites sur les racines de P , soit on fait appel à la question précédente). Alors, $|z_0 - w| = |w| \leq 1$. Donc P vérifie $\mathcal{IS}(z_0)$.

2. Cas d'une racine de module 1

On note t_1, \dots, t_{n-1} les racines complexes non nécessairement distinctes de P' . Ainsi,

$$P' = na_n \prod_{i=1}^{n-1} (X - t_i).$$

On suppose que $n_0 = 1$.

- (a) La décomposition en éléments simples de $\frac{P''}{P'}$ est :

$$\frac{P''}{P'} = \sum_{i=1}^{n-1} \frac{1}{X - t_i}.$$

En effet, remarquez que si une racine est de multiplicité α , elle contribuera pour α termes de la somme précédente, et on retrouve ainsi le terme $\frac{\alpha}{X - t}$ de la décomposition exprimée avec les multiplicités.

Supposons que $\left| \frac{P''}{P'}(z_0) \right| \geq n - 1$ (ce qui a un sens puisque z_0 est racine simple de P , donc non racine de P') donc que

$$\left| \sum_{i=1}^{n-1} \frac{1}{z_0 - t_i} \right| \geq n - 1.$$

Par inégalité triangulaire, on en déduit que

$$\sum_{i=1}^{n-1} \frac{1}{|z_0 - t_i|} \geq n - 1.$$

Alors (raisonnement par l'absurde immédiat), au moins un terme de cette somme doit être plus grand que 1. Il existe donc $i \in \llbracket 1, n - 1 \rrbracket$ tel que $\frac{1}{|z_0 - t_i|} \geq 1$, donc $|z_0 - t_i| \leq 1$. Cela nous assure bien que

P vérifie $\mathcal{IS}(z_0)$.

- (b) Soit Q tel que $P = (X - z_0)Q$. On a alors :

$$P' = (X - z_0)Q' + Q \quad \text{et} \quad P'' = (X - z_0)Q'' + 2Q'.$$

En évaluant en z_0 , il vient donc

$$\frac{P''}{P'}(z_0) = \frac{2Q'}{Q}(z_0).$$

Or, $Q = \prod_{i=1}^m (X - z_i)^{n_i}$, donc la décomposition en éléments simples de Q est :

$$\frac{Q'}{Q} = \sum_{i=1}^m \frac{n_i}{X - z_i}.$$

On obtient donc bien la relation attendue :

$$\frac{P''}{P'}(z_0) = 2 \sum_{i=1}^m \frac{n_i}{z_0 - z_i}.$$

(c) Soit $z \in \mathbb{C}$ tel que $|z| \leq 1$, et $z \neq 1$. Alors

$$\begin{aligned} \operatorname{Re}\left(\frac{1}{1-z}\right) &= \frac{1}{2} \left(\frac{1}{1-z} + \frac{1}{1-\bar{z}} \right) \\ &= \frac{1}{2} \cdot \frac{2-z-\bar{z}}{(1-z)(1-\bar{z})} \\ &= \frac{1}{2} \cdot \frac{2-2\operatorname{Re}(z)}{1+|z|^2-2\operatorname{Re}(z)}. \end{aligned}$$

Or, $0 < |1-z|^2 = 1+|z|^2-2\operatorname{Re}(z) \leq 2-2\operatorname{Re}(z)$, donc $\boxed{\operatorname{Re}\left(\frac{1}{1-z}\right) \geq \frac{1}{2}}$

(d) On suppose $z_0 = 1$. Comme les z_i sont différents de z_0 pour $i \in \llbracket 1, m \rrbracket$, et de module au plus 1, d'après la question précédente,

$$\forall i \in \llbracket 1, n-1 \rrbracket, \operatorname{Re}\left(\frac{1}{z_0 - z_i}\right) \geq \frac{1}{2}.$$

Ainsi, il découle de la question II-2(b) que :

$$\operatorname{Re}\left(\frac{P''}{P'}(z_0)\right) \geq 2 \sum_{i=1}^m \frac{n_i}{2} = \sum_{i=1}^m n_i = n-1.$$

Or, en utilisant la décomposition en éléments simples de $\frac{P''}{P'}$,

$$\frac{P''}{P'} = \sum_{i=1}^{n-1} \frac{1}{z_0 - t_i}.$$

Ainsi,

$$\sum_{i=1}^{n-1} \operatorname{Re}\left(\frac{1}{z_0 - t_i}\right) \geq n-1.$$

Cette somme étant constituée de $n-1$ termes, au moins un terme doit être plus grand que 1. Il existe donc

$i \in \llbracket 1, n-1 \rrbracket$ tel que $\boxed{\operatorname{Re}\left(\frac{1}{1-t_i}\right) \geq 1}$ (on rappelle que $z_0 = 1$)

Or, pour tout $z \in \mathbb{C}$, $\operatorname{Re}(z) \leq |z|$, donc on déduit de ce qui précède que $\frac{1}{|1-t_i|} \geq 1$, donc que $\boxed{|1-t_i| \leq 1}$.

On en déduit que $\boxed{P \text{ vérifie } \mathcal{IS}(1)}$.

(e) On considère $\tilde{P} = P(z_0 X)$. Si on écrit $z_0 = e^{i\theta}$, cela revient à faire une rotation d'angle θ avant d'appliquer P . On a alors :

$$\tilde{P}(X) = a_n \prod_{i=0}^m (z_0 X - z_i)^{n_i} = a'_n \prod_{i=0}^m \left(X - \frac{z_i}{z_0}\right)^{n_i},$$

où $a'_n = a_n z_0^n$. Ainsi, les racines de \tilde{P} sont les $\frac{z_i}{z_0}$, de même multiplicité n_i . En particulier, toutes les racines de \tilde{P} sont aussi de module au plus 1.

Puisque $\tilde{P}'(X) = z_0 P'(z_0 X)$, une description similaire est aussi valide pour les racines de \tilde{P}' en fonction des racines de P .

En particulier, 1 est racine simple de \tilde{P} , et d'après 2(d), \tilde{P} vérifie $\mathcal{IS}(1)$. Il existe donc une racine $\tilde{\zeta}$ de \tilde{P}' telle que $|1 - \tilde{\zeta}| \leq 1$. Or, $\tilde{\zeta}$ s'écrit sous la forme $\tilde{\zeta} = \frac{\zeta}{z_0}$, pour une certaine racine de P' . Puisque z_0 est de module 1, on a alors

$$1 \geq |1 - \tilde{\zeta}| = \left|1 - \frac{\zeta}{z_0}\right| = |z_0 - \zeta|.$$

Ainsi, $\boxed{P \text{ vérifie } \mathcal{IS}(z_0)}$.

Partie III – Cas des polynômes de degrés 3 et 4

1. Étude de T

- (a) Pour commencer, montrons que pour tout $w \in \mathbb{C} \setminus \frac{1}{a}$, on peut appliquer T à $T(w)$, donc que $T(w) \neq \frac{1}{a}$. En effet :

$$T(w) - \frac{1}{a} = \frac{aw - a^2 - aw + 1}{a(aw - 1)} = \frac{1 - a^2}{a(aw - 1)} \neq 0.$$

Ainsi, la composition est licite, et

$$T \circ T(w) = \frac{\frac{w-a}{aw-1} - a}{a \cdot \frac{w-a}{aw-1} - 1} = \frac{w - a - a^2w + a}{aw - a^2 - aw + 1} = \frac{(1 - a^2)w}{1 - a^2} = w.$$

Ainsi, $T \circ T = \text{id}_{\mathbb{C} \setminus \{\frac{1}{a}\}}$.

- (b) Soit $|w| = 1$. On a alors

$$|T(w)|^2 = \frac{(w-a)(\bar{w}-a)}{(aw-1)(a\bar{w}-1)} = \frac{|w|^2 + a^2 - a(w+\bar{w})}{|w|^2 a^2 + 1 - a(w+\bar{w})} = \frac{1 + a^2 - a(w+\bar{w})}{1 + a^2 - a(w+\bar{w})} = 1.$$

Ainsi, $|T(w)| = 1$.

- (c) La question précédente nous assure que $T(\mathbb{U}) \subset \mathbb{U}$. Réciproquement, soit $w \in \mathbb{U}$. Alors $w = T(T(w))$, et en posant $z = T(w) \in \mathbb{U}$ (d'après la question précédente), il vient $w = T(z)$, donc $w \in T(\mathbb{U})$. Ainsi, $\mathbb{U} \subset T(\mathbb{U})$, et les deux inclusions amènent $T(\mathbb{U}) = \mathbb{U}$.

Soit alors w tel que $|w| \neq 1$, et $w \neq \frac{1}{a}$. Soit $z = T(w)$. Si $|z| = 1$, d'après ce qui précède, il existe $w' \in \mathbb{U}$ tel que $T(w') = z$, donc $T(w') = T(w)$. Comme $|w| \neq 1$, on a alors $w \neq w'$, ce qui implique que T n'est pas injective. Cela contredit la bijectivité de T , découlant de l'identité $T \circ T = \text{id}_{\mathbb{C} \setminus \{\frac{1}{a}\}}$ (T est son propre inverse).

Ainsi, $|T(w)| \neq 1$.

- (d) Soit w tel que $|w| < 1$. Soit $f : t \mapsto |T(tw)|$, continue sur $[0, 1]$ en tant que composée de fonctions continues (fonction polynomiale, module), à valeurs dans \mathbb{R}_+ . On a $f(0) = |T(0)| = a < 1$, et $f(1) = |T(w)|$. Si $|T(w)| \geq 1$, d'après le théorème des valeurs intermédiaires, il existe $t \in]0, 1[$ tel que $f(t) = 1$, donc $T(tw) = 1$. Or, $|tw| < 1$, donc une telle égalité contredit le résultat de la question III-1(c). Par conséquent, $|T(w)| < 1$.

- (e) On a donc $T(B(0, 1)) \subset B(0, 1)$, et le même argument que pour \mathbb{U} montre que $T(B(0, 1)) = B(0, 1)$.

Ainsi, $T(\overline{B}(0, 1)) = \overline{B}(0, 1)$, et comme T est injective, les éléments de $\overline{B}(0, 1)$ ne peuvent donc pas être l'image d'un autre élément, hors que $\overline{B}(0, 1)$. On en déduit que si $|w| > 1$, alors $|T(w)| > 1$.

Le résultat global obtenu dans cette question III-1 est en fait lié à des propriétés de connexité, que vous étudierez l'année prochaine.

2. (a) Il suffit d'explicitier \tilde{P} à l'aide des coefficients de P :

$$\tilde{P}(X) = (aX - 1)^n \sum_{i=0}^n a_i \left(\frac{X-a}{aX-1} \right)^i = \sum_{i=0}^n a_i (X-a)^i (aX-1)^{n-i}.$$

Il s'agit donc bien d'un élément de $\mathbb{C}[X]$ en tant que combinaison linéaire de polynômes à coefficients complexes. Ainsi, $\tilde{P} \in \mathbb{C}[X]$.

- (b) Soit $w \in \mathbb{C}$, différent de $\frac{1}{a}$; w est racine de \tilde{P} si et seulement si $P(T(w)) = 0$, donc si $T(w)$ est racine de P ; cela implique en particulier que $|T(w)| \leq 1$, et la contraposée de III-1(e) permet de conclure que $|w| \leq 1$.

On conclut en remarquant que $\frac{1}{a}$ n'est pas racine de \tilde{P} . En effet, en évaluant l'expression trouvée dans la question précédente,

$$\tilde{P}\left(\frac{1}{a}\right) = a_n \left(\frac{1}{a} - a\right)^n \neq 0.$$

Ainsi, toutes les racines de \tilde{P} sont de module au plus 1.

- (c) On remarque que $\tilde{P}(0) = P(a) = 0$ par hypothèse. Notons $w_0 = 0, w_1, \dots, w_{n-1}$ les racines non nécessairement distinctes de \tilde{P} (qui est de degré n).

On a alors, d'après les relations de Viète (relations coefficients/racines) :

$$\left| \frac{b_{n-1}}{b_n} \right| = \left| \sum_{i=0}^{n-1} w_i \right| = \left| \sum_{i=1}^{n-1} w_i \right| \leq \sum_{i=1}^{n-1} |w_i| \leq n - 1.$$

Ainsi, $\boxed{|b_{n-1}| \leq (n-1)|b_n|}$.

De même,

$$\left| \frac{b_1}{b_n} \right| = |\Sigma_{n-1}(w_0, \dots, w_{n-1})|,$$

où Σ_{n-1} désigne le polynôme symétrique élémentaire à n variables de degré $n-1$, c'est-à-dire la somme de tous les produits de $n-1$ des n racines. Ces produits contiennent tous la racine $w_0 = 0$, sauf le produit des $n-1$ dernières racines. Ainsi, seul le terme correspondant à ce produit reste dans la somme, et il vient :

$$\left| \frac{b_1}{b_n} \right| = \left| \prod_{i=1}^{n-1} w_i \right| \leq 1,$$

soit : $\boxed{|b_1| \leq |b_n|}$.

3. (a) On remarque que les notations sont bien définies, puisque R est de degré $n-1$: en effet, l'unique terme de degré n intervenant dans sa définition est précédé d'un coefficient nul, et le coefficient du terme de degré $n-1$ est

$$A = b_{n-1} + n \frac{b_n}{a},$$

qui est non nul, sinon on aurait $|b_{n-1}| = \frac{n}{a}|b_n| > (n-1)|b_n|$, contredisant ainsi la question III-2(c).

Ce coefficient est alors le coefficient dominant de R , intervenant dans la décomposition donnée dans l'énoncé.

On applique encore les relations de Viète : en notant c le coefficient constant de R , le produit des racines est égal, au signe près, à $\frac{c}{R}$. Or :

$$c = \frac{b_1}{a},$$

donc, en utilisant la question III-2(c) :

$$\prod_{k=1}^{n-1} |\gamma_k| = \frac{|b_1|/a}{|b_{n-1} + n \frac{b_n}{a}|} \leq \frac{|b_n|}{|ab_{n-1} + nb_n|} = \frac{1}{\left| a \frac{b_{n-1}}{b_n} + a \right|}$$

Or,

$$\left| a \frac{b_{n-1}}{b_n} + n \right| \geq n - a \left| \frac{b_{n-1}}{b_n} \right| \geq n - a(n-1) > 0,$$

donc

$$\boxed{\prod_{k=1}^{n-1} |\gamma_k| \leq \frac{1}{n - a(n-1)}}.$$

- (b) On calcule l'expression de droite :

$$\begin{aligned} na\tilde{P}(X) - (aX-1)\tilde{P}'(X) &= \sum_{i=0}^n nab_i X^i - \sum_{i=1}^n aib_i X^i + \sum_{i=1}^n ib_i X^{i-1} \\ &= a \sum_{i=1}^n \left((n-i)b_i X^i + \frac{ib_i}{a} X^{i-1} \right) = aR(X), \end{aligned}$$

la deuxième égalité venant du fait que $b_0 = 0$, puisque 0 est racine de \tilde{P} .

- (c) Par définition,

$$P(T(X)) = \frac{\tilde{P}(X)}{(aX-1)^n}.$$

En dérivant, on obtient :

$$T'(X)P'(T(X)) = \frac{\tilde{P}'(X)}{(aX-1)^n} - na \frac{\tilde{P}(X)}{(aX-1)^{n+1}}.$$

Puisque

$$T'(X) = \frac{aX-1-a(X-a)}{(aX-1)^2} = \frac{a^2-1}{(aX-1)^2},$$

il vient, après simplifications :

$$P'(T(X)) = \frac{1}{(a^2 - 1)(aX - 1)^{n-1}} \left((aX - 1)\tilde{P}'(X) - na\tilde{P}(X) \right) = \frac{-aR(X)}{(a^2 - 1)(aX - 1)^{n-1}}.$$

En évaluant en w , on obtient bien :

$$\boxed{P'(T(w)) = \frac{a}{(1 - a^2)(aw - 1)^{n-1}} \cdot R(w)}.$$

(d) Soit μ un nombre réel tel que $|\gamma_1| \leq \mu < \frac{1}{a}$. D'après la question précédente, $\zeta = T(\gamma_1)$ est racine de P' , et vérifie :

$$|\zeta - a| = |T(\gamma_1) - a| = \left| \frac{\gamma_1 - a - a(a\gamma_1 - 1)}{a\gamma_1 - 1} \right| = \left| \frac{(1 - a^2)\gamma_1}{a\gamma_1 - 1} \right| \leq \frac{(1 - a^2)\mu}{|a\gamma_1 - 1|}.$$

Or, $|a\gamma_1 - 1| \geq 1 - a|\gamma_1| \geq 1 - a\mu > 0$, donc

$$\boxed{|\zeta - a| \leq \frac{(1 - a^2)\mu}{1 - a\mu}}$$

(e) On remarquera que $\frac{1}{1 + a - a^2} \leq \frac{1}{a}$, puisque $1 - a^2 \geq 0$. Ainsi, cette inégalité est plus forte que la majoration précédente. Supposons donc $\mu \leq \frac{1}{1 + a - a^2}$. Puisque

$$1 - a\mu \geq 1 - \frac{a}{1 + a - a^2} = \frac{1 - a^2}{1 + a - a^2} > 0,$$

on peut écrire :

$$|\zeta - a| \leq \frac{\mu(1 - a^2)(1 + a - a^2)}{1 - a^2} = \mu(1 + a - a^2) \leq 1.$$

Ainsi, P' a une racine ζ vérifiant $\boxed{|\zeta - a| \leq 1}$, donc P vérifie $\mathcal{IS}(a)$.

4. Le cas $n = 2$ a déjà été étudié. On se contente donc des cas $n = 3$ et $n = 4$. D'après la question précédente, il suffit de montrer que $|\gamma_1| \leq \frac{1}{1 + a - a^2}$. On pourra alors bien trouver μ comme dans la question précédente, nous assurant que P vérifie $\mathcal{IS}(a)$.

Or, le classement des racines $|\gamma_k|$ et la question III-3(a) nous assurent qu'il suffit de montrer que $\frac{1}{n - a(n - 1)} \leq \frac{1}{(1 + a - a^2)^{n-1}}$. En effet, dans ce cas, on aura :

$$|\gamma_1|^{n-1} \leq \prod_{i=1}^{n-1} |\gamma_k| \leq \frac{1}{n - a(n - 1)} \leq \frac{1}{(1 + a - a^2)^{n-1}},$$

ce qui nous assure $|\gamma_1| \leq \frac{1}{1 + a - a^2}$ et nous permet de conclure.

En appliquant le logarithme croissant, il suffit de montrer que $(n - 1) \ln(1 + a - a^2) \leq \ln(n - a(n - 1))$. On étudie donc la fonction $f : x \mapsto (n - 1) \ln(1 + x - x^2) - \ln(n - (n - 1)x)$ sur $[0, 1]$. Puisque $f(1) = 0$, il suffit de montrer que f est croissante sur $[0, 1]$.

Pour cela on exprime la dérivée de f sur $[0, 1]$:

$$\forall x \in [0, 1], f'(x) = \frac{(n - 1)(1 - 2x)}{1 + x - x^2} + \frac{n - 1}{n - (n - 1)x} = (n - 1) \cdot \frac{(n - (n - 1)x)(1 - 2x) - (1 + x - x^2)}{(1 + x - x^2)(n - (n - 1)x)}.$$

Il suffit donc de prouver la positivité de $(n - (n - 1)x)(1 - 2x) + (1 + x - x^2)$ sur $[0, 1]$.

On étudie les deux cas $n = 3$ et $n = 4$:

- Pour $n = 3$, on obtient le trinôme $(3 - 2x)(1 - 2x) + 1 + x - x^2 = 4 - 7x + 3x^2 = (x - 1)(3x - 4)$. Comme ses racines sont 1 et $\frac{4}{3}$, il est positif sur $[0, 1]$, d'où la conclusion.
- Pour $n = 4$, on obtient le trinôme $(4 - 3x)(1 - 2x) + 1 + x - x^2 = 5 - 10x + 5x^2 = 5(1 - x)^2 \geq 0$, d'où également la conclusion voulue.

Ainsi, lorsque $n \leq 4$, $\boxed{P \text{ vérifie } \mathcal{IS}(a)}$.

5. Soit z une racine de P :

- si z est racine multiple de P , P vérifie $\mathcal{IS}(z)$ d'après I-2.
- si z est racine simple de module 1, P vérifie $\mathcal{IS}(z)$ d'après II-2(e)
- si z est racine simple de module strictement inférieur à 1, une rotation comme en II-2(e) nous permet de nous ramener à la question III-4, et P vérifie encore $\mathcal{IS}(z)$.

Ainsi, si $n \leq 4$, P vérifie $\mathcal{IS}(z)$ pour chacune de ses racines, donc $\boxed{P \text{ vérifie } \mathcal{IS}}$.

Partie IV – Cas des polynômes de degré 5, 6, 7 avec une racine double de module 1

1. Soit P admettant un zéro réel $z_0 = a \in]0, 1[$, et un zéro au moins double w de module 1. Pour commencer remarquons qu'on peut se contenter d'étudier le cas où $n_0 = 1$ (sinon, on conclut avec I-2). Puisque $w \neq \frac{1}{a}$, et $T^{-1}(w) = T(w)$ est bien définie, et est un zéro au moins double de \tilde{P} , d'après ce qui précède. On en déduit que $T(w)$ est un zéro \tilde{P}' , et d'après III-3(b), $T(w)$ est racine de R . De plus, puisque $T(\mathbb{U}) = \mathbb{U}$, le module de $T(w) = 1$. L'une des racines de R étant de module 1 et les $n - 2$ autres de module supérieur ou égal à $|\gamma_1|$, on obtient cette fois

$$|\gamma_1|^{n-2} \leq \frac{1}{n - a(n-1)}.$$

Le même raisonnement qu'en III-4 nous assure qu'il suffit alors de montrer la croissance de la fonction $g : x \mapsto (n-2)\ln(1+x-x^2) - \ln(n - (n-1)x)$, donc la positivité de sa dérivée

$$x \mapsto \frac{(n-2)(1-2x)}{1+x-x^2} + \frac{(n-1)}{n - (n-1)x} = \frac{(n-2)(n - (n-1)x)(1-2x) + (n-1)(1+x-x^2)}{(n - (n-1)x)(1+x-x^2)}.$$

Il suffit donc d'étudier le signe du numérateur. On l'exprime explicitement pour chaque valeur de $n = 5, 6$ ou 7. C'est un travail un peu laborieux mais sans difficulté théorique.

- Cas $n = 5$: le numérateur est : $x \mapsto 13 - 20x + 8x^2$. Pour déterminer sans trop de calculs le signe du discriminant, notez la petite astuce suivante (encore plus utile dans les cas suivants, qui sinon nous donnent des multiplications un peu pénibles) :

$$\Delta = 20^2 - 4 \times 13 \times 8 = 20^2 - (20-4)(20+6) = -2 \times 20 + 24 < 0.$$

Ainsi le numérateur est toujours positif.

- Cas $n = 6$: le numérateur est : $x \mapsto 29 - 63x + 35x^2$, de discriminant :

$$\Delta = 63^2 - 4 \times 29 \times 35 = 63^2 - (63-5)(63+7) = -2 \times 63 + 35 < 0,$$

et on arrive à la même conclusion.

- cas $n = 7$: le numérateur est : $x \mapsto 41 - 94x + 54x^2$, de discriminant

$$\Delta = 94^2 - (94-12)(94+14) = -2 \times 94 + 13 \times 14 = -6 < 0,$$

et on arrive encore une fois à la bonne conclusion.

Ainsi, lorsque $n = 5, 6$ ou 7 et P possède au moins une racine double de module 1 et une racine réelle dans $]0, 1[$, $\boxed{P \text{ vérifie } \mathcal{IS}(a)}$.

2. Le même argument de rotation qu'en II-3(e) montre alors que si P de degré 5, 6 ou 7 possède une racine multiple de module 1 et toute ses racines de module inférieur à 1, alors pour toute racine z de module strictement plus petit que 1, P vérifie $\mathcal{IS}(z)$. C'est aussi le cas pour les racines de module 1 d'après la partie II, on en déduit que $\boxed{P \text{ vérifie } \mathcal{IS}}$.

Partie V – Continuité des racines d'un polynôme

1. • Supposons que $S_k \rightarrow S$. Pour tout $i \in \llbracket 0, n \rrbracket$, et tout $k \in \mathbb{N}$,

$$0 \leq |s_{i,k} - s_i| \leq \|S_k\| \xrightarrow{k \rightarrow +\infty} 0.$$

Ainsi, d'après le théorème d'encadrement, $\boxed{\lim_{k \rightarrow +\infty} s_{i,k} = s_i}$.

- Réciproquement, si pour tout $i \in \llbracket 0, n \rrbracket$, $s_{i,k} \rightarrow s_i$, alors

$$\lim_{k \rightarrow +\infty} \|S_k - S\| = \sum_{i=0}^n \lim_{k \rightarrow +\infty} |s_{i,k} - s_i| = 0.$$

Donc $S_k \rightarrow S$.

Ainsi, $S_k \rightarrow S$ ssi pour tout $i \in \llbracket 0, n \rrbracket$, $s_{i,k} \rightarrow s_i$.

- Supposons que $S_k \rightarrow S$. Alors à z fixé dans \mathbb{C} , d'après la question précédente, $s_{i,k}z^i \rightarrow s_i z^i$, donc, en prenant la somme finie de ces limites, il vient :

$$\lim_{k \rightarrow +\infty} S_k(z) = \sum_{i=0}^n \lim_{k \rightarrow +\infty} s_{i,k}z^i = \sum_{i=0}^n s_i z^i = S(z).$$

- Si $|z| \leq 1$, on a évidemment $|z| \leq 1 \leq \frac{\|S\|}{|s_n|}$;
 - Si $|z| \geq 1$, puisque $S(z) = 0$, on a

$$|s_n z^n| = \left| \sum_{k=0}^{n-1} s_k z^k \right| \leq \sum_{k=0}^{n-1} |s_k z^k|.$$

En divisant par $|z^{n-1}| \geq 1 > 0$,

$$|s_n z| \leq \sum_{k=0}^{n-1} |s_k| |z|^{n-1-k},$$

Et comme pour tout $k \in \llbracket 0, n-1 \rrbracket$, $|z|^{n-1-k} \leq 1$, il vient :

$$|s_n z| \leq \sum_{k=0}^{n-1} |s_k| \leq \sum_{k=0}^n |s_k| = \|S\|.$$

Ainsi, on a bien obtenu : $|z| \leq \frac{\|S\|}{|s_n|}$.

- Soit $(S_k)_{k \in \mathbb{N}}$ une suite de polynômes de degré n convergeant vers S de degré n . On note $S_k = \alpha_k \prod_{i=1}^n (X - x_{i,k})$.

- Puisque $S_k \rightarrow S$, on a convergence coefficient par coefficient, donc $\|S_k\| \rightarrow \|S\|$, et $s_{n,k} \rightarrow s_n \neq 0$. Ainsi,

$$\frac{\|S_k\|}{|s_{n,k}|} \rightarrow \frac{\|S\|}{s_n}.$$

On en déduit que la suite $\left(\frac{\|S_k\|}{|s_{n,k}|}\right)$ est bornée, disons majorée par un réel M . La question V-3 nous assure alors que toutes les racines de tous les S_k ont un module majoré par M . Par conséquent, chacune des suites

$(x_{i,k})_{k \in \mathbb{N}}$ est bornée.

- D'après le théorème de Bolzano-Weierstass pour les complexes, on peut extraire une suite convergente $(x_{1,\varphi(k)})$ de $(x_{1,k})$. La suite $(x_{2,\varphi(k)})$ est bornée et on peut donc en extraire une suite convergente $(x_{2,\varphi \circ \psi(k)})$. La suite $(x_{1,\varphi \circ \psi(k)})$ est bien sûr encore convergente, puisqu'extraite de la suite convergente $(x_{1,\varphi(k)})$. En composant de la sorte les extractions, on extrait successivement des suites convergentes de chaque $(x_{i,k})$, tout en préservant la convergence des précédentes. On obtient donc finalement une extractrice Φ assurant la convergence de toutes les suites de racine : pour tout $i \in \llbracket 1, n \rrbracket$, $(x_{i,\Phi(k)})$ converge, vers une limite x_i .

La suite $(S_{\Phi(k)})$ répond alors à la question.

- On raisonne par l'absurde, en supposant qu'il existe $\varepsilon > 0$, et ζ racine de S de multiplicité β pour tout K , il existe $k \geq K$ tel que $B(\zeta, \varepsilon)$ contient strictement moins de β racines de S_k . On se donne un tel ε et un tel ζ . Pour $K = 0$, on trouve $k_1 \geq 0$ tel que $B(\zeta, \varepsilon)$ contient moins de β racines de S_{k_1} . Pour $K = k_1 + 1$, on trouve $k_2 \geq K > k_1$ vérifiant la même propriété, puis $k_3 \geq k_2 + 1 > k_2$ etc. On construit ainsi par récurrence une suite extraite de $(S_k)_{k \in \mathbb{N}}$ en ne gardant que les indices k_i ainsi construits. Tous les polynômes de cette suite extraite ont strictement moins de β racines dans la boule $B(\zeta, \varepsilon)$. Notons $(T_k) = (S_{\varphi(k)})$ cette suite extraite, et numérotons (arbitrairement) $y_{i,k}$, $i \in \llbracket 1, n \rrbracket$ les racines de T_k . D'après la question précédente, on

peut extraire de (T_k) une suite $(T_{\psi(k)})$ telle que les suites $(y_{i,\psi(k)})$ soient toutes convergentes, disons vers y_i . Notons de plus a_k le coefficient dominant de T_k et a celui de S . La question V-1 nous assure que $a_k \rightarrow a$. Ainsi, pour tout $z \in \mathbb{C}$,

$$T_{\varphi(k)}(z) = a_k \prod_{i=1}^n (z - y_{i,k}) \xrightarrow{k \rightarrow +\infty} a \prod_{i=1}^n (z - y_i).$$

Ceci étant vrai pour tout z de \mathbb{C} (donc une infinité de valeurs), et la limite de $T_{\varphi(k)}$ étant S (point par point d'après V-2), on en déduit que

$$S(X) = a \prod_{i=1}^n (X - y_i)$$

Or, il ne peut pas y avoir β des complexes y_i égaux à ζ , sinon à partir d'un certain rang, les β suites correspondantes $(y_{i,k})$ prendraient leurs valeurs dans $B(\zeta, \varepsilon)$, contredisant la construction de (T_k) . Ainsi, on obtient une contradiction sur le fait que ζ est racine de multiplicité β de S .

On en conclut que pour tout $\varepsilon > 0$ et toute racine ζ de multiplicité β , à partir d'un certain rang, $B(\zeta, \varepsilon)$ contient β racines de S_k .

- (d) On peut choisir ε suffisamment petit pour que les boules de rayon ε centrées en chacune des racines de S n'aient pas d'intersection, par exemple en prenant

$$\varepsilon < \frac{1}{2} \min(|\zeta_1 - \zeta_2|, \zeta_1 \neq \zeta_2 \in \text{Rac}(S)).$$

Alors il existe K tel que pour tout $k \geq K$, chaque boule $B(\zeta, \varepsilon)$ contient $\beta(\zeta)$ racines de S_k , $\beta(\zeta)$ étant la multiplicité de ζ . Les boules étant distinctes, cela fournit $\sum_{\zeta \in \text{Rac}(S)} \beta(\zeta)$ racines de S_k , c'est-à-dire n . Comme S_k ne peut pas avoir plus de racine, aucune des boules $B(\zeta, \varepsilon)$ ne peut contenir strictement plus de $\beta(\zeta)$ racines de S_k .

Par conséquent, $B(\zeta, \varepsilon)$ contient exactement $\beta(\zeta)$ racines de S_k .

Partie VI – Polynômes extrémaux

1. (a) Soit $S \in P_n(k)$. Soit z une racine de S . Comme $n \geq 2$, S' admet au moins une racine ζ , également dans $\overline{B}(0, 1)$ d'après II-1(b). Alors

$$|z - \zeta| \leq |z| + |\zeta| \leq 2.$$

Ainsi, $I_S(z) \leq 2$, et ceci étant vrai pour toute racine z de S , $I(S) \leq 2$.

En considérant $S = X^n - 1$, S est unitaire, admet n racines distinctes $e^{i \frac{2k\pi}{n}}$, de module 1, et S' a 0 comme unique racine. Ainsi, $S \in P_n(n-1)$, et de façon immédiate, pour chacune de ses racines, $I_S(z) = |z - 0| = 1$, donc $I(S) = 1$.

On note $I(P_k(n))$ la borne supérieure des $I(S)$ lorsque S parcourt $P_n(k)$.

- (b) Supposons que $I(P_n(k)) \leq 1$. Soit alors $S \in P_n(k)$. Par définition, $I(S) \leq 1$, donc pour tout $z \in \text{rac}(S)$, $I_S(z) \leq 1$. Or, il existe une racine ζ de S' telle que

$$|z - \zeta| = I_S(z) \leq 1.$$

On en déduit que S vérifie $\mathcal{IS}(z)$, et ceci pour tout z racine de S . Donc S vérifie \mathcal{IS} .

- (c) Soit (S_m) une suite d'éléments de $P_n(k)$, S_m étant de coefficients $s_{i,m}$, $i \in \llbracket 0, n \rrbracket$. Les relations de Viète et le fait que les racines des S_m sont toutes de module 1 nous assurent que les suites $(s_{i,m})_k$ sont toutes bornées. Une extraction simultanée construite comme en V-4(b) nous permet d'extraire de (S_m) une suite $(S_{\text{phi}(m)})$ telle que les suites de coefficient $(s_{i,\varphi(m)})$ soient toutes convergentes, disons de limite s_i . Ainsi, d'après V-1, $(S_{\varphi(m)})$ converge vers

$$S = \sum_{i=0}^n s_i X^i.$$

Par ailleurs, la question V-4(c) nous assure que toute racine de S est limite d'une suite de racines des $S_{\varphi(m)}$. Ces racines étant toutes de module au plus 1, il en est donc de même des racines de S .

Enfin, si S admet strictement plus de $k + 1$ racines, en notant $\zeta_1, \dots, \zeta_{k+2}$ des racines distinctes de S , et ε suffisamment petit pour que les boules $B(\zeta_i, \varepsilon)$ n'aient pas d'intersections, la question V-4(d) nous donne, à partir d'un certain rang, l'existence d'au moins une racine de S_m dans chacune des boules $B(\zeta_i, \varepsilon)$, donc strictement plus de $k + 1$ racines de S_m , ce qui contredit l'appartenance de S_m à $P_n(k)$. Ainsi, S admet au plus $k + 1$ racines distinctes.

On en déduit que $S \in P_n(k)$. Ainsi, on a réussi à extraire de (S_m) une suite convergeant dans $P_n(k)$. Par conséquent, $P_n(k)$ est compact.

- (d) Cela provient de la question V-4(d) assurant que si $(S_m) \rightarrow S$, alors les racines de S_m sont proches des racines de S . De plus, la question V-1 nous assure que $S'_m \rightarrow S'$, donc que cette propriété est également vérifiée pour les racines des polynômes dérivés.

Utilisons le critère séquentiel. Soit $S_m \rightarrow S$, et donc $S'_m \rightarrow S'$. D'après les résultats de la partie IV, pour tout ε suffisamment petit, et tout m assez grand, les racines de S sont toutes comprises dans des boules de rayon $\frac{\varepsilon}{2}$ centrées en les racines de S , chacune de ces boules contenant au moins une racine de S_m , et de même pour les racines de S'_m . Soit $\varepsilon > 0$, suffisamment petit pour que cette propriété soit vérifiée, et K tel que cette description soit vraie pour tout $m \geq K$. Soit $m \geq K$.

- Soit alors z_m une racine de S_m , et z une racine de S telle que $z_m \in B(z, \frac{\varepsilon}{2})$. Soit ζ_0 tel que $|z - \zeta_0|$ soit minimal, égal à $I_S(z)$. Il existe ζ_m une racine de S'_m dans $B(\zeta_0, \frac{\varepsilon}{2})$. Alors, par inégalité triangulaire, $|z_m - \zeta_m| \leq I_S(z) + \varepsilon$, donc $I_S(z_m) \leq I_S(z) + \varepsilon \leq I(S) + \varepsilon$.
On en déduit que pour tout $m \geq K$, $I(S_m) \leq I(S) + \varepsilon$.
- Soit maintenant z réalisant le maximum de $I_S(z)$. D'après V-4(c), pour tout $m \geq K$, il existe z_m une racine de S_m telle que $z_m \in B(z, \frac{\varepsilon}{2})$. Toute racine ζ_m de S'_m est dans une boule $B(\zeta, \frac{\varepsilon}{2})$, pour une certaine racine ζ de S' . Alors, par inégalité triangulaire,

$$|z_m - \zeta_m| \geq |z - \zeta| - \varepsilon \geq I_S(z) - \varepsilon = I(S) - \varepsilon.$$

Cette inégalité étant vraie pour toute racine ζ_m de S'_m , il vient que $I_{S_m}(z_m) \geq I(S) - \varepsilon$, puis en prenant le maximum sur les racines de S_m , $I(S_m) \geq I(S) - \varepsilon$.

- Ainsi, pour tout $m \geq K$, $|I(S_m) - I(S)| \leq \varepsilon$. On en déduit que $I(S_m) \rightarrow I(S)$. ceci étant vrai pour toute suite (S_m) convergeant vers S , on en déduit, d'après le critère séquentiel, que I est une application continue de $P_n(k)$ dans \mathbb{R} .
- D'après le théorème de compacité, il existe donc un polynôme S de $P_n(k)$ réalisant le maximum de la fonction I sur le compact $P_n(k)$, donc tel que $I(S) = I(P_n(k))$.

2. On appelle polynôme extrémal de $P_n(k)$ un polynôme S de $P_n(k)$ vérifiant $I(S) = I(P_n(k))$.

- (a) Si ce n'est pas le cas, soit $\lambda \in [0, 1[$ le module maximal d'une racine de S . On définit $T(X) = S(\lambda X)$ (cela revient à faire une homothétie). Alors z' est racine de T si et seulement s'il existe z racine de S tel que $z' = \lambda z$. En particulier, λ majorant le module des racines de S , les racines de T sont de module inférieur à 1, et en nombre égal au nombre de racines (distinctes) de P . Ainsi, $T \in P_k(n)$

Par ailleurs, $T'(X) = \lambda S'(\lambda X)$, et les racines de T' sont obtenues par la même transformation à partir des racines de S' . Ainsi, pour toute racine z' de T et ζ' de T' , il existe des racines z de S et ζ de S' tel que $|z' - \zeta'| = \frac{1}{\lambda}|z - \zeta|$, et inversement. Par conséquent, $I(T) = \frac{1}{\lambda}I(S) > I(S)$. Cela contredit l'extrémalité de S .

Ainsi, un polynôme extrémal a au moins une racine de module 1.

- (b) Soit S extrémal.

Supposons qu'il n'existe aucune racine de la forme $e^{i\alpha}$, pour $\alpha \in [\theta, \theta + \pi[$. Le nombre de racines étant fini, il existe donc $\varepsilon > 0$ tel que pour tout $\alpha \in [\theta, \theta + \pi + \varepsilon[$, $e^{i\alpha}$ ne soit pas racine de S . Quitte à faire une rotation d'angle $-\theta - \frac{\varepsilon}{2}$ (c'est à dire considérer $S(z_0 X)$, pour un certain complexe de module 1), du fait que la rotation conserve les distances (entre les racines de S , et de S'), donc l'extrémalité, on peut se ramener au cas où S n'a pas de racine de la forme $e^{i\alpha}$, pour $\alpha \in [-\frac{\varepsilon}{2}, \pi + \frac{\varepsilon}{2}[$, donc en particulier, pas de racine sur la partie supérieure du cercle trigonométrique.

Pour toute racine z_i de S , on peut alors trouver ε_i tel que pour tout $x \in [0, \varepsilon_i[$, $|z_i + ix| < 1$ (en montant un tout petit peu, on ne sort pas de la boule unité, puisqu'on n'est pas sur son bord supérieur, et en montant

encore moins, on reste dans la boule ouverte). Soit alors ε le minimum des ε_i , pour l'ensemble des racines de S .

On compose alors par une translation qui relève les racines de ε , en considérant $T(X) = S(X - i\varepsilon)$. Ainsi, z' est racine de T si et seulement si $z' - i\varepsilon$ est racine de S , donc s'il existe une racine z de S tel que $z' = z + \varepsilon$. Le choix de ε nous assure que les racines de T sont toutes de module strictement inférieur à 1. La description des racines de T nous assure qu'il y en a autant que les racines de S , donc au plus $k + 1$. Ainsi, $T \in P_n(k)$. De plus, la translation étant une isométrie, et agissant également comme telle sur les racines de T et de T' , on a $I(S) = I(T)$, donc T est extrémal, et ne possède aucune racine de module 1. Cela contredit la question précédente.

Ainsi, $\boxed{S \text{ possède une racine dans chaque demi-cercle unité}}$.

(c) On suppose $n = 5, 6$ ou 7 et $k = 3$. On note S un polynôme extrémal de $P_n(k)$. On suppose que S a une racine a réelle vérifiant $0 < a < 1$. D'après la question précédente, S admet au moins deux racines distinctes de module 1.

- Si a est racine multiple, S vérifie $\mathcal{IS}(a)$ d'après I-2.
- Si l'une des racines de module 1 est multiple, alors S vérifie \mathcal{IS} d'après IV-2, donc $\mathcal{IS}(a)$.
- On peut donc supposer que a est racine simple, et toutes les racines de module 1 sont simples. Alors, S ne peut pas avoir 3 racines de module 1, puisque, S ayant au maximum 4 racines distinctes, S n'aurait que 4 racines simples, donc serait de degré au plus 4. Ainsi, S possède exactement 2 racines de module 1. D'après la question précédente, elles sont nécessairement diamétralement opposées. On les note u et $v = -u$. Soit b la quatrième racine, de multiplicité $n - 3$. On a alors

$$S = (X - u)(X - v)(X - a)(X - b)^{n-3}.$$

De plus, b est racine de multiplicité $n - 4$ de S' , dont le degré est $n - 1$. Ainsi, S' a trois autres racines ζ_1, ζ_2 et ζ_3 non nécessairement distinctes. On a

$$S' = n(X - b)^{n-4}(X - \zeta_1)(X - \zeta_2).$$

Ainsi,

$$|S'(a)| = n|a - b|^{n-4}|a - \zeta_1| \cdot |a - \zeta_2| \cdot |a - \zeta_3|, \quad \text{donc:} \quad |a - \zeta_1| \cdot |a - \zeta_2| \cdot |a - \zeta_3| = \frac{1}{n}S'(a)|a - b|^{4-n}.$$

Or, en dérivant $S = (X - u)(X - v)(X - a)(X - b)^{n-3}$ et en évaluant en a , il vient :

$$S'(a) = (a - u)(a - v)(a - b)^{n-3}.$$

Ainsi, pour ζ racine de S' la plus proche de a (égale à b, ζ_1, ζ_2 ou ζ_3), on obtient :

$$|a - \zeta|^3 \leq |a - \zeta_1| \cdot |a - \zeta_2| \cdot |a - \zeta_3| = \frac{1}{n}|a - u| \cdot |a - v| \cdot |a - b| \leq \frac{2}{n}|a - u| \cdot |a - v|$$

Pour terminer, on calcule :

$$|a - u||a - v| = |(a - u)(a + u)| = |a^2 - u^2| \leq a^2 + |u|^2 \leq 2;$$

Ainsi, puisque $n \geq 5$, $|a - \zeta|^3 \leq \frac{4}{n}$, donc $|a - \zeta| \leq 1$.

On en déduit donc bien que $\boxed{S \text{ vérifie } \mathcal{IS}(a)}$.

(d) On suppose $n = 5, 6$ ou 7 , et S extrémal dans $P_n(3)$.

- Si z est une racine de module 1, d'après la partie I, S vérifie $\mathcal{IS}(z)$.
- Si $0 < |z| < 1$, par rotation, on se ramène au cas d'une racine réelle $a \in]0, 1[$, et donc S vérifie $\mathcal{IS}(z)$ d'après ce qui précède.
- Si $z = 0$, alors S vérifie $\mathcal{IS}(z)$ d'après la partie II.

Ainsi, $\boxed{S \text{ vérifie } \mathcal{IS}}$.

On en déduit que $I(S) \leq 1$, donc que $\boxed{I(P_n(3)) \leq 1}$.

3. • Si $n = 2, 3, 4$, cela résulte des parties I et III
- Si $n = 5, 6, 7$, cela provient de la question précédente et de VI-1(b)
- Si $n \geq 8$, et si S a $m \leq 4$ racines distinctes, alors $n \geq 2^m$, et le résultat découle de I-3(c).

Ainsi, $\boxed{\text{tout polynôme ayant au plus 4 racines distinctes, toutes de module au plus 1, vérifie } \mathcal{IS}}$.