DM 20 : polynômes cyclotomiques et nombres de Salem [corrigé]

Notations

On notera respectivement $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ les corps des nombres complexes, réels et rationnels, $\mathbb{Z}$ l'anneau des entiers relatifs, et $\mathbb{N}$ l'ensemble des entiers naturels.

Pour un entier $n \geqslant 1$ on dit qu'un nombre complexe z est une *racine n-ième de l'unité* si $z^n = 1$, et que z est une *racine de l'unité* s'il existe $k \geqslant 1$ tel que z soit une racine k-ième de l'unité.

Pour $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ on notera $R[X]$ l'anneau des polynômes à coefficients dans R. Un polynôme non nul est *unitaire* si son coefficient dominant est égal à 1.

On notera $\mathbb{C}(X)$ le corps des fractions de $\mathbb{C}[X]$. Pour $F \in \mathbb{C}(X)$ n'ayant pas 0 comme pôle et un entier k, on notera $\text{coeff}_k(F) = \dfrac{F^{(k)}(0)}{k!}$.

Un polynôme $P \in \mathbb{Q}[X]$ est *irréductible dans* $\mathbb{Q}[X]$ si P n'est pas constant et si l'égalité $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ implique que Q ou R est constant.

Un nombre complexe x est appelé *nombre algébrique* s'il existe $P \in \mathbb{Q}[X]$ non nul tel que $P(x) = 0$. On dit que $x \in \mathbb{C}$ est un *entier algébrique* s'il existe $P \in \mathbb{Z}[X]$ **unitaire** tel que $P(x) = 0$.

On admet le résultat suivant.

> **Théorème.** L'ensemble des entiers algébriques est un sous-anneau de $\mathbb{C}$.

Le problème est consacré à l'étude des polynômes unitaires de $\mathbb{Z}[X]$, irréductibles dans $\mathbb{Q}[X]$ et qui possèdent beaucoup de racines de module 1.

La partie 1 est préliminaire et utilisée en fin de parties 2 et 3. La partie 3 est indépendante de la partie 2. La partie 4 utilise les notions introduites précédemment mais est, à l'exception des questions 19 et 20, indépendante du reste.

Partie 1.

Le but de cette partie est d'introduire les notions de polynôme minimal et de degré d'un nombre algébrique, et de montrer que le polynôme minimal d'un entier algébrique est à coefficients entiers.

Dans les questions 1 à 4, on fixe un nombre algébrique α. Soit

$$I(\alpha) = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}.$$

1. Montrer que $I(\alpha)$ est un idéal de $\mathbb{Q}[X]$, différent de $\{0\}$.

   On peut vérifier rapidement que :
   - $0 \in I(\alpha)$;
   - $\forall P, Q \in I(\alpha), P + Q \in I(\alpha)$;
   - $\forall P \in I(\alpha), \forall R \in \mathbb{Q}[X], PR \in I(\alpha)$.

   (Le troisième point montrera aussi $\forall P \in I(\alpha), -P \in I(\alpha)$, que l'on n'a donc pas inclus dans la liste.)

   On va procéder de manière un peu différente, en vérifiant que l'application $\text{év}_\alpha : \begin{cases} \mathbb{Q}[X] \to \mathbb{C} \\ P \mapsto P(\alpha) \end{cases}$ *est un morphisme d'anneaux, puis en en déduisant que* $I(\alpha) = \ker \text{év}_\alpha$ *est un idéal de* $\mathbb{Q}[X]$.

- *Soit* $P, Q \in \mathbb{Q}[X]$. *On a*

$$\begin{aligned} \text{év}_\alpha(P+Q) &= (P+Q)(\alpha) = P(\alpha) + Q(\alpha)\,; \\ \text{év}_\alpha(PQ) &= (PQ)(\alpha) = P(\alpha)\,Q(\alpha)\,; \\ \text{év}_\alpha(1) &= 1, \end{aligned}$$

  Donc év_α *est un morphisme d'anneaux.*

- *De manière générale, montrons que le noyau* $\ker\varphi$ *d'un morphisme d'anneaux* $\varphi : A \to B$ *est un idéal de* A.
  - *Comme un morphisme d'anneaux est en particulier un morphisme de groupes,* $\ker\varphi$ *est un sous-groupe de* A.
  - *Soit* $x \in \ker\varphi$ *et* $y \in A$. *On a* $\varphi(xy) = \underbrace{\varphi(x)}_{=0}\,\varphi(y) = 0$, *donc* $xy \in \ker\varphi$.

  Cela montre que $\ker\varphi$ *est un idéal de* A.
  En particulier, $I(\alpha) = \ker \text{év}_\alpha$ *est un idéal de* $\mathbb{Q}[X]$.
- *Le fait que* α *soit algébrique signifie exactement* $I(\alpha) \neq \{0\}$.

Il existe donc un unique polynôme unitaire Π_α, *appelé* polynôme minimal *de* α, *tel que*

$$I(\alpha) = \{\Pi_\alpha Q \mid Q \in \mathbb{Q}[X]\}\,.$$

On appelle degré de α *le degré du polynôme* Π_α.

2. Montrer que α est de degré 1 si et seulement si $\alpha \in \mathbb{Q}$.

   - *Supposons* α *de degré* 1. *Son polynôme minimal* Π_α *est donc unitaire, de degré* 1, *et possède* α *comme racine, donc* $\Pi_\alpha = X - \alpha$.
     Comme $\Pi_\alpha \in \mathbb{Q}[X]$, *on a* $\alpha \in \mathbb{Q}$.
   - *Réciproquement, supposons* $\alpha \in \mathbb{Q}$. *On a donc déjà* $X - \alpha \in I(\alpha)$, *donc* $\Pi_\alpha \mid X - \alpha$.
     Si Π_α *était constant, on aurait* $\Pi_\alpha = 1$, *ce qui est impossible, car* $1 \notin I(\alpha)$.
     Le polynôme minimal Π_α *est donc un diviseur unitaire non constant de* $X - \alpha$, *d'où* $\Pi_\alpha = X - \alpha$ *et donc* $\deg(\alpha) = \deg\Pi_\alpha = 1$.

3. (a) Montrer que Π_α est irréductible dans $\mathbb{Q}[X]$.

   Soit $Q, R \in \mathbb{Q}[X]$ *tels que* $\Pi_\alpha = QR$.
   En évaluant en α, *il vient* $Q(\alpha)R(\alpha) = \Pi_\alpha(\alpha) = 0$. *Comme* $\mathbb{C}$ *est intègre, on en déduit* $Q(\alpha) = 0$ *ou* $R(\alpha) = 0$, *c'est-à-dire* $\Pi_\alpha \mid Q$ *(auquel cas les polynômes* Π_α *et* Q *seraient associés, donc* R *serait de degré nul) ou* $\Pi_\alpha \mid R$ *(auquel cas* Q *serait de degré nul).*
   Cela montre l'irréductibilité de Π_α.

   (b) Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire, irréductible dans $\mathbb{Q}[X]$. Montrer que si z est une racine complexe de P, alors P est le polynôme minimal de z.

   Supposons que z *est une racine complexe de* P.
   On a $P \in I(z)$, *donc* Π_z *divise* P *: on peut donc trouver* $Q \in \mathbb{Q}[X]$ *tels que* $\Pi_z Q = P$. *Comme* P *est irréductible et que* $\deg P_z > 0$ *(comme on l'a vu à la question 2), on en déduit* $\deg Q = 0$, *c'est-à-dire que* P *et* Π_z *sont associés.*
   Comme ils sont tous deux unitaires, on en déduit $P = \Pi_z$.

4. (a) Soient $A, B \in \mathbb{Q}[X]$ deux polynômes qui possèdent une racine commune dans $\mathbb{C}$. Montrer que A et B ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.

Le PGCD $A \wedge B$ est le même, qu'on le calcule dans $\mathbb{Q}[X]$ ou dans $\mathbb{C}[X]$.
Si l'on note $\alpha \in \mathbb{C}$ une racine complexe commune à A et à B, le polynôme complexe $X - \alpha$ divise donc à la fois A et B, donc il divise $A \wedge B$.
On a donc $\deg(A \wedge B) \geqslant 1$, ce qui montre que A et B ne sont pas premiers entre eux.

(b) Montrer que les racines de Π_α dans $\mathbb{C}$ sont simples.

Si Π_α possédait une racine multiple $\alpha \in \mathbb{C}$, on aurait $\Pi_\alpha(\alpha) = \Pi'_\alpha(\alpha) = 0$ donc Π_α et Π'_α ne seraient pas premiers entre eux, d'après la question précédente.
Comme Π_α est irréductible, cela devrait entraîner $\Pi_\alpha \mid \Pi'_\alpha$, ce qui est impossible pour des raisons de degré.

5. (a) Montrer que si $\alpha \in \mathbb{Q}$ est un entier algébrique, alors $\alpha \in \mathbb{Z}$.

Soit $\alpha \in \mathbb{Q}$ un entier algébrique, $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux tels que $\alpha = \dfrac{p}{q}$, et $P = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$ un polynôme unitaire à coefficients entiers dont α est racine.
En chassant les dénominateurs, il vient $p^d + a_{d-1}\, p^{d-1}\, q + \cdots + a_1\, p\, q^{d-1} + a_0\, q^d = 0$. On a donc $\ell \nmid p^d$ (d'après une conséquence du lemme de Gauss) et $\ell \mid a_{d-1}\, p^{d-1}\, q + \cdots + a_1\, p\, q^{d-1} + a_0\, q^d$, ce qui est une contradiction, puisque ces deux nombres sont opposés.

(b) Montrer que si $\alpha \in \mathbb{C}$ est un entier algébrique, alors $\Pi_\alpha \in \mathbb{Z}[X]$.
Indication : utiliser le théorème admis en introduction ainsi que la question 5a.

Soit $\alpha \in \mathbb{C}$ un entier algébrique. On peut donc trouver un polynôme unitaire $P \in \mathbb{Z}[X]$ dont α est racine, et on a automatiquement que Π_α divise P dans $\mathbb{Q}[X]$.
En particulier, toutes les racines de Π_α sont des racines de P, et donc des entiers algébriques.
On écrit la décomposition en facteurs irréductibles

$$\Pi_\alpha = \prod_{j=1}^{d} (X - \alpha_j)$$

de son polynôme minimal, où $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$.
D'après les relations coefficients-racines, pour tout $k \in [\![0, d-1]\!]$, le coefficient de degré $d - k$ de Π_α est

$$(-1)^k \sum_{1 \leqslant j_1 < \cdots < j_k \leqslant d} \alpha_{j_1} \cdots \alpha_{j_k},$$

qui est un entier algébrique d'après le résultat admis par l'énoncé.
Par ailleurs, comme $\Pi_\alpha \in \mathbb{Q}[X]$, ces coefficients sont des nombres rationnels. On en déduit, d'après la question précédente, qu'il s'agit d'entiers relatifs.
Comme le coefficient de degré d de ce polynôme vaut par ailleurs 1, on a bien montré que $\Pi_\alpha \in \mathbb{Z}[X]$.

6. (a) Soit $\alpha \in \mathbb{C}$ un entier algébrique de degré 2 et de module 1. Montrer que α est une racine de l'unité.

- *Si α était réel, il vaudrait ± 1 à cause de l'hypothèse sur son module. Cela contredit l'information $\deg(\alpha) = 2$ car $\deg(\pm 1) = 1$ d'après 2.*
- *Ainsi, $\alpha \notin \mathbb{R}$. Comme $\Pi_\alpha \in \mathbb{Z}[X] \subseteq \mathbb{R}[X]$, on en déduit que $\overline{\alpha}$ est également racine de Π_α, ce qui entraîne $\Pi_\alpha = (X - \alpha)(X - \overline{\alpha})$.*

► *En particulier, le coefficient de degré* 1 *de* Π_α *vaut* $-\alpha - \overline{\alpha} = -2\,\mathrm{Ré}(\alpha)$. *Le nombre* $2\,\mathrm{Ré}(\alpha)$ *est donc un réel compris entre* -2 *et* 2 *(car* $\forall z \in \mathbb{C}, |\mathrm{Ré}(z)| \leqslant |z|$*) mais aussi un nombre entier, ce qui laisse très peu de choix.*

- *On ne peut pas avoir* $2\,\mathrm{Ré}(\alpha) = \pm 2$, *car cela entraînerait* $\mathrm{Ré}(\alpha) = \pm 1$ *et donc* $\alpha = \pm 1$, *cas que nous avons déjà exclu.*
- *Si* $2\,\mathrm{Ré}(\alpha) = -1$, *on a* $\{\alpha, \overline{\alpha}\} = \{j, \bar{j}\}$.
- *Si* $2\,\mathrm{Ré}(\alpha) = 0$, *on a* $\{\alpha, \overline{\alpha}\} = \{i, \bar{i}\}$;
- *Enfin, si* $2\,\mathrm{Ré}(\alpha) = 1$, *on a* $\{\alpha, \overline{\alpha}\} = \{\zeta_6, \overline{\zeta}_6\}$, *où* $\zeta_6 = \exp\left(i\frac{2\pi}{6}\right)$.

Dans tous les cas, α *est bien une racine (et même une racine douzième) de l'unité.*

(b) Montrer que $\dfrac{3+4i}{5}$ est un nombre algébrique de degré 2 et de module 1 mais n'est pas une racine de l'unité.

Le nombre $\alpha = \dfrac{3+4i}{5}$ *est racine de*

$$P = (X - \alpha)(X - \overline{\alpha}) = X^2 - \frac{6}{5}X + 1,$$

qui est un polynôme irréductible de $\mathbb{R}[X]$ *(c'est un polynôme du second degré sans racine réelle), donc* $P = \Pi_\alpha$.
Comme $P \notin \mathbb{Z}[X]$, *la question 5b entraîne que* α *n'est pas un entier algébrique.*

Partie 2.

Le but de cette partie est de caractériser les polynômes unitaires $P \in \mathbb{Z}[X]$, *irréductibles dans* $\mathbb{Q}[X]$, *dont toutes les racines sont de module* 1.

Pour n *un entier supérieur ou égal à* 1 *on dit qu'une racine* n*-ième de l'unité* z *est* primitive *si* $z^d \neq 1$ *pour tout entier* d *tel que* $1 \leqslant d < n$. *On note* $\mathbb{P}_n$ *l'ensemble des racines primitives* n*-ièmes de l'unité. On a donc* $\mathbb{P}_1 = \{1\}$. *On définit* $\Phi_n \in \mathbb{C}[X]$ *par*

$$\Phi_n = \prod_{z \in \mathbb{P}_n} (X - z).$$

Si a *et* b *sont des entiers, on écrit* $a \mid b$ *si* a *divise* b.

7. Montrer que pour tout $n \geqslant 1$ on a

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

le produit étant pris sur l'ensemble des entiers $d > 0$ divisant n.

On peut reformuler la définition en disant que $\mathbb{P}_n$ *est l'ensemble des éléments du groupe multiplicatif* $\mathbb{C}^\times$ *qui sont exactement d'ordre* n.
D'après le théorème de Lagrange, tout élément de $\mathbb{U}_n$ *possède un certain ordre, qui est un diviseur de* n. *On a donc* $\mathbb{U}_n = \bigsqcup_{d \mid n} \mathbb{P}_d$, *où il est clair que l'union est disjointe.*
On en déduit

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d \mid n} \prod_{\omega \in \mathbb{P}_d} (X - \omega) = \prod_{d \mid n} \Phi_d.$$

8. (a) Montrer que si p est un nombre premier et $k \geqslant 1$ est un entier, alors

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

À l'aide de la question précédente, on remarque que

$$X^{p^k} - 1 = \prod_{d|p^k} \Phi_d = \prod_{i=0}^{k} \Phi_{p^i} = \left(\prod_{i=0}^{k-1} \Phi_{p^i}\right) \Phi_{p^k} = \left(X^{p^{k-1}} - 1\right) \Phi_{p^k}.$$

On remarque (par intégrité de $\mathbb{C}[X]$) qu'il existe un unique polynôme vérifiant cette relation.
Or,

$$\left(X^{p^{k-1}} - 1\right)\left(X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1\right) = X^{p^k} - 1,$$

par le même calcul que celui donnant la somme des termes d'une suite géométrique.
Ainsi, $\Phi^{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1$.

(b) Calculer Φ_n pour $n = 1, 2, 3, 4, 5, 6$.

La question précédente couvre tous les cas à l'exception de $n = 1$ (qui est facile car $\mathbb{P}_1 = \{1\}$) et $n = 6$, que l'on obtient en vérifiant que $\mathbb{P}_6 = \left\{\zeta_6, \overline{\zeta}_6\right\}$, et donc $\Phi_6 = (X - \zeta_6)(X - \overline{\zeta}_6)$. On obtient :

$$\Phi_1 = X - 1 \qquad \Phi_4 = X^2 + 1$$
$$\Phi_2 = X + 1 \qquad \Phi_5 = X^4 + X^3 + X^2 + X + 1$$
$$\Phi_3 = X^2 + X + 1 \qquad \Phi_6 = X^2 - X + 1.$$

On fixe un entier $n \geqslant 2$ pour toute la suite de cette partie.

9. (a) Calculer $\Phi_n(0)$.

On a déjà $\Phi_1(0) = -1$.
Pour tout $n \geqslant 2$, notons $A(n)$ l'assertion $\Phi_n(0) = 1$.
Montrons $\forall n \geqslant 2, A(n)$ par récurrence forte.

Hérédité. *Soit $n \geqslant 2$ tel que $\forall d \in [\![2, n-1]\!], A(d)$. Montrons $A(n)$.*
(On remarque que quand $n = 2$, l'hypothèse que l'on vient de faire est vide, ce qui explique que l'on n'ait pas besoin d'initialiser la récurrence...)
On a, d'après la question 7, $X^n - 1 = \prod_{d|n} \Phi_d = (X-1)\left(\prod_{\substack{d|n \\ 2 \leqslant d \leqslant n-1}} \Phi_d\right)\Phi_n$.
En évaluant en 0, il vient (d'après l'hypothèse de récurrence)

$$-1 = -1 \times \left(\prod_{\substack{d|n \\ 2 \leqslant d \leqslant n-1}} \underbrace{\Phi_d(1)}_{=1}\right) \times \Phi_n(1),$$

d'où $\Phi_n(1) = 1$, ce qui clôt la récurrence.
On a donc ($\Phi_1(0) = -1$ et) $\forall n \geqslant 2, \Phi_n(0) = 1$.

(b) Calculer $\Phi_n(1)$ en fonction de la décomposition en facteurs premiers de n.
Indication : raisonner par récurrence sur n, en utilisant la question 7.

On a déjà $\Phi_1(1) = 0$ et, d'après la question 8a, pour tout nombre premier p et tout exposant $k \geqslant 1$, $\Phi_{p^k}(1) = p$.
La relation 7 se réécrit par ailleurs, pour tout $n \geqslant 2$,

$$X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1 = \prod_{\substack{d|n \\ d\geqslant 2}} \Phi_d,$$

ce qui donne notamment, après évaluation en 1,

$$n = \prod_{\substack{d|n \\ 2\leqslant d}} \Phi_d(1). \tag{✠}$$

Pour tout $n \geqslant 2$, notons $A(n)$ l'assertion $\Phi_n(1) = \begin{cases} p & \text{si } n \text{ est une puissance d'un premier } p \\ 1 & \text{sinon.} \end{cases}$

Montrons $\forall n \geqslant 2, A(n)$ par récurrence forte.

Hérédité. *Soit $n \geqslant 2$ tel que $\forall d \in [\![2, n-1]\!], A(d)$. Montrons $A(n)$.*

- *Si n est une puissance d'un nombre premier, on a déjà le résultat.*
- *Supposons donc que n n'est pas la puissance d'un nombre premier. On peut donc écrire $n = p_1^{k_1} \cdots p_r^{k_r}$, où $p_1 < \cdots < p_r$ sont des nombres premiers et $k_1, \ldots, k_r \in \mathbb{N}^*$.*
  Les diviseurs (différents de 1) de n se décomposent alors en deux types :
  - *les $p_i^{\ell_i}$, pour un certain $i \in [\![1, r]\!]$ et $\ell_i \in [\![1, k_i]\!]$ (notons que, comme n n'est pas une puissance d'un nombre premier, ces diviseurs sont tous $\leqslant n-1$) : pour un tel diviseur, on a $\Phi_{p_i^{\ell_i}}(1) = p_i$;*
  - *les autres diviseurs d, parmi lesquels n lui-même : à part le cas $d = n$, on sait déjà que pour eux, $\Phi_d(1) = 1$.*

  On a alors

$$\begin{aligned} \prod_{\substack{d|n \\ 2\leqslant d\leqslant n-1}} \Phi_d(1) &= \prod_{i=1}^{r} \prod_{\ell=1}^{k_i} \Phi_{p_i^\ell}(1) \times \prod_{\substack{d|n \\ 2\leqslant d\leqslant n-1 \\ d\neq p^*}} \Phi_d(1) \\ &= \prod_{i=1}^{r} \prod_{\ell=1}^{k_i} p_i \qquad \text{(hyp. de récurrence)} \\ &= \prod_{i=1}^{r} p_i^{k_i} = n, \end{aligned}$$

  où le deuxième produit de la première ligne court sur les diviseurs (stricts) de n qui ne sont pas des puissances de nombres premiers.
  En comparant avec (✠), on en déduit $\Phi_n(1) = 1$.

Cela clôt la récurrence.

10. Montrer que $\Phi_n \in \mathbb{Z}[X]$.

- *Commençons par montrer que si l'on a l'égalité $AB = C$ avec $A \in \mathbb{Z}[X]$ unitaire, $B \in \mathbb{C}[X]$ et $C \in \mathbb{Z}[X]$, alors en fait $B \in \mathbb{Z}[X]$.*

*(Autrement dit, quand on effectue la division euclidienne d'un polynôme à coefficients entiers par un polynôme **unitaire** à coefficients entiers, le quotient est encore à coefficients entiers – c'est assez clair si l'on « pose » la division euclidienne, mais on va le démontrer plus formellement).*

Soit A, B *et* C *trois tels polynômes. On note* $a = \deg A \in \mathbb{N}$ *et* $b = \deg B$ *(le cas* $B = 0$ *étant trivial, on peut également supposer* $b \in \mathbb{N}$*.)*

Avant de nous lancer dans la démonstration proprement dite, notons que l'énoncé a redéfini la notation coeff_k *(en l'étendant à certaines fractions rationnelles), mais que, grâce à la formule de Taylor, pour un polynôme* $P \in \mathbb{C}[X]$, $\mathrm{coeff}_k(P)$ *continue à designer le* k*-ième coefficient de* P*.*

Nous allons maintenant montrer $\forall k \in [\![0, b]\!], \mathrm{coeff}_k(B) \in \mathbb{Z}$ *par récurrence finie descendante forte.*

Initialisation. *On a* $\underbrace{\mathrm{coeff}_{a+b}(C)}_{\in\mathbb{Z}} = \mathrm{coeff}_a(A)\,\mathrm{coeff}_b(B) = \mathrm{coeff}_b(B)$*, d'où* $\mathrm{coeff}_b(B) \in \mathbb{Z}$*.*

Hérédité. *Soit* $k \in [\![0, b]\!]$ *tel que* $\forall \ell > k, \mathrm{coeff}_\ell(B) \in \mathbb{Z}$*. Montrons* $\mathrm{coeff}_k(B) \in \mathbb{Z}$*.*

On a (car $a + k - j < 0$ *dès que* $j < k$*)*

$$\mathrm{coeff}_{a+k}(C) = \sum_{\substack{i\leqslant a\\ j\leqslant b\\ i+j=a+k}} \mathrm{coeff}_i(A)\,\mathrm{coeff}_j(B) = \sum_{j=k}^{b} \mathrm{coeff}_{a+k-j}(A)\,\mathrm{coeff}_j(B),$$

ce qui donne

$$\mathrm{coeff}_k(B) = \mathrm{coeff}_{a+k}(C) - \sum_{j=k+1}^{b} \mathrm{coeff}_{a+k-j}(A)\,\underbrace{\mathrm{coeff}_j(B)}_{\in\mathbb{Z}} \in \mathbb{Z},$$

et clôt la récurrence.

- *On peut maintenant se lancer dans la question proprement dite. La question 7 montre que*

$$X^n - 1 = \Phi_n \times \left(\prod_{\substack{d|n\\ d\neq n}} \Phi_d \right).$$

Puisqu'il est clair que tous les polynômes Φ_d *sont unitaires, si l'on savait en outre que les* Φ_d*, pour* $d < n$*, étaient à coefficients entiers, le point précédent montrerait que* Φ_n *l'est aussi.*

Comme $\Phi_1 = X - 1$ *est bel et bien à coefficients entiers, une récurrence forte assez immédiate conclut alors.*

Soit $P \in \mathbb{Z}[X]$ *un polynôme unitaire de degré* $n \geqslant 1$*, irréductible dans* $\mathbb{Q}[X]$ *et dont toutes les racines complexes sont de module* 1*. L'objectif des questions 11 et 12 est de montrer que toutes les racines de* P *sont des racines de l'unité.*

Soient $z_1, \ldots, z_n$ *les racines complexes de* P *comptées avec leurs multiplicités, de sorte que*

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

Pour tout entier $k \geqslant 0$ *on note*

$$a_k = z_1^k + z_2^k + \cdots + z_n^k.$$

11. Soient $\mathcal{E}$ l'ensemble des fractions rationnelles $F \in \mathbb{C}(X)$ n'admettant pas 0 comme pôle et $\mathcal{E}_\mathbb{Z} = \{F \in \mathcal{E} \mid \forall k \in \mathbb{N}, \mathrm{coeff}_k(F) \in \mathbb{Z}\}$.

(a) Montrer que $\mathcal{E}$ et $\mathcal{E}_{\mathbb{Z}}$ sont des sous-anneaux de $\mathbb{C}(X)$.

- *L'inclusion $\mathcal{E}_{\mathbb{Z}} \subseteq \mathcal{E}$ est automatique.*
- *On a clairement $1 \in \mathcal{E}_{\mathbb{Z}}$ (et donc $1 \in \mathcal{E}$).*
- *La stabilité de $\mathcal{E}$ par différence est immédiate, celle de $\mathcal{E}_{\mathbb{Z}}$ découle directement de*

$$\forall F, G \in \mathcal{E}, \forall k \in \mathbb{N}, \operatorname{coeff}_k(F - G) = \operatorname{coeff}_k(F) - \operatorname{coeff}_k(G).$$

- *La stabilité de $\mathcal{E}$ par produit est immédiate, celle de $\mathcal{E}_{\mathbb{Z}}$ provient du fait que, pour tous $F, G \in \mathcal{E}$ et $k \in \mathbb{N}$, on a*

$$\begin{aligned}
\operatorname{coeff}_k(FG) &= \frac{(FG)^{(k)}(0)}{k!} \\
&= \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} F^{(i)}(0)\, G^{(k-i)}(0) && \textit{(formule de Leibniz)} \\
&= \sum_{i=0}^{k} \frac{F^{(i)}(0)}{i!} \frac{G^{(k-i)}(0)}{(k-i)!} \\
&= \sum_{i=0}^{k} \operatorname{coeff}_i(F)\ \operatorname{coeff}_{k-i}(G).
\end{aligned}$$

(b) Soit $D \in \mathbb{Z}[X]$ tel que $D(0) = 1$. Montrer que D est un élément inversible de $\mathcal{E}_{\mathbb{Z}}$.

La démonstration est presque la même que celle de la question 10.

Notons $C = \dfrac{1}{D} \in \mathbb{Q}(X)$. Puisque $D(0) \neq 0$, on a $C \in \mathcal{E}$. La relation obtenue à la question précédente montre que

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} \operatorname{coeff}_k(C) \operatorname{coeff}_{n-k}(D) = \delta_{n,0}.$$

Montrons alors par récurrence forte que $\forall k \in \mathbb{N}, \operatorname{coeff}_k(C) \in \mathbb{Z}$, ce qui conclura.

Initialisation. *On a $\operatorname{coeff}_0(C) = \operatorname{coeff}_0(C) \operatorname{coeff}_0(D) = 1 \in \mathbb{Z}$.*

Hérédité. *Soit $k \in \mathbb{N}^*$ tel que $\forall j \in [\![0, k-1]\!], \operatorname{coeff}_j(C) \in \mathbb{Z}$. Montrons $\operatorname{coeff}_k(C) \in \mathbb{Z}$. On a*

$$0 = \delta_{k,0} = \sum_{j=0}^{k} \operatorname{coeff}_j(C) \operatorname{coeff}_{k-j}(D),$$

donc

$$\operatorname{coeff}_k(C) = \operatorname{coeff}_k(C) \operatorname{coeff}_0(D) = -\sum_{j=0}^{k-1} \operatorname{coeff}_j(C) \operatorname{coeff}_{k-j}(D) \in \mathbb{Z},$$

ce qui clôt la récurrence.

Remarquons d'ailleurs qu'essentiellement la même preuve montrerait que le groupe des inversibles de $\mathcal{E}_{\mathbb{Z}}$ est $\{F \in \mathcal{E}_{\mathbb{Z}} \mid F(0) = \pm 1\}$.

(c) Montrer que $X^n P\left(\dfrac{1}{X}\right)$ est un élément inversible de $\mathcal{E}_{\mathbb{Z}}$ et en déduire l'existence de $F \in \mathcal{E}_{\mathbb{Z}}$ telle que

$$X F(X) P\left(\frac{1}{X}\right) = P'\left(\frac{1}{X}\right).$$

- *Si* $Q = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$ *est un polynôme de degré* d*, on a*

$$X^d Q\left(\frac{1}{X}\right) = X^d \left(\frac{a_d}{X^d} + \frac{a_{d-1}}{X^{d-1}} + \cdots + \frac{a_1}{X} + a_0\right) = a_d + a_{d-1} X + \cdots + a_1 X^{d-1} + a_0 X^d,$$

qui est un polynôme de degré au plus d*, ayant les mêmes coefficients (dans un autre ordre) que* Q*.*

- *Le calcul précédent montre même que le coefficient dominant de* Q *est le coefficient constant de* $X^d Q\left(\frac{1}{X}\right)$*.*
- *En particulier, comme* P *est un polynôme unitaire de degré* n *à coefficients entiers, on a que* $X^n P\left(\frac{1}{X}\right)$ *est un polynôme à coefficients entiers, de degré* $\leqslant n$ *et de coefficient constant* 1*. D'après la question précédente, il s'agit donc d'un élément inversible de* $\mathcal{E}_{\mathbb{Z}}$*.*
- *Pour les mêmes raisons,* $X^{n-1} P'\left(\frac{1}{X}\right)$ *est un polynôme à coefficients entiers, de degré* $\leqslant n-1$*, et est donc un élément de* $\mathcal{E}_{\mathbb{Z}}$*.*
- *La fraction rationnelle*

$$F = \frac{X^{n-1} P'\left(\frac{1}{X}\right)}{X^n P\left(\frac{1}{X}\right)} = \frac{P'\left(\frac{1}{X}\right)}{X P\left(\frac{1}{X}\right)}$$

est donc un élément de $\mathcal{E}_{\mathbb{Z}}$*, ce qui équivaut à l'égalité demandée.*

(d) Obtenir une expression explicite de F sous forme d'une somme finie et en déduire que $\forall k \in \mathbb{Z}, a_k \in \mathbb{Z}$.

On connait la décomposition en éléments simples de $\frac{P'}{P}$ *:*

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

En composant par $\frac{1}{X}$*, il vient*

$$F(X) = \frac{1}{X}\left(\frac{P'}{P} \circ \frac{1}{X}\right) = \sum_{i=1}^{n} \frac{1}{1 - z_i X}.$$

Or, $\frac{1}{1 - z_i X} \in \mathcal{E}$ *et un calcul direct montre que pour tout* $k \in \mathbb{N}$*, on a*

$$\left(\frac{1}{1 - z_i X}\right)^{(k)} = \frac{k!\, z_i^k}{(1 - z_i X)^{k+1}} \qquad \text{et donc} \qquad \operatorname{coeff}_k\left(\frac{1}{1 - z_i X}\right) = z_i^k.$$

On en déduit $\forall k \in \mathbb{N}, \operatorname{coeff}_k(F) = \sum_{i=1}^{n} z_i^k = a_k$*, et* $F \in \mathcal{E}_{\mathbb{Z}}$ *entraîne alors* $\forall k \in \mathbb{N}, a_k \in \mathbb{Z}$*.*

12. (a) Montrer qu'il existe deux entiers $0 \leqslant k < \ell$ tels que $a_{k+i} = a_{\ell+i}$ pour tout $i \in \{0, 1, \ldots, n\}$. On fixe deux tels entiers k, ℓ dans les questions 12b et 12c.

- *On a, pour tout* $p \in \mathbb{N}$*,*

$$|a_p| = \left|\sum_{i=1}^{n} z_i^p\right| \leqslant \sum_{i=1}^{n} \underbrace{|z_i|^p}_{=1} = n.$$

► *L'application*

$$\begin{cases} \mathbb{N} \to & [\![-n, n]\!]^{n+1} \\ k \mapsto & (a_k, \dots, a_{k+n}) \end{cases}$$

a pour domaine un ensemble infini et pour codomaine un ensemble fini. D'après la version infinie du principe des tiroirs, elle ne peut donc pas être injective, ce qui conclut.

(b) Montrer que $\sum_{i=1}^{n} F(z_i)(z_i^\ell - z_i^k) = 0$ pour tout polynôme $F \in \mathbb{C}[X]$ de degré inférieur ou égal à n.

L'application $\varphi : \begin{cases} \mathbb{C}_n[X] \to & \mathbb{C} \\ F \quad \mapsto & \sum_{i=1}^{n} F(z_i)(z_i^\ell - z_i^k) \end{cases}$ *est clairement linéaire.*

Par définition de k *et* ℓ*, on a, pour tout* $j \in [\![0, n]\!]$*,*

$$\varphi(X^j) = \sum_{i=1}^{n} \left(z_i^{\ell+j} - z_i^{k+j} \right) = a_{\ell+j} - a_{k+j} = 0.$$

La fonction φ *est donc nulle sur la base canonique de* $\mathbb{C}_n[X]$*. Par prolongement des identités, elle est nulle, ce qui conclut.*

(c) Montrer que $z_1, z_2, \dots, z_n$ sont deux à deux distincts. En déduire que $z_i^{\ell-k} = 1$ pour tout $i \in \{1, 2, \dots, n\}$ et conclure.

► *Comme* P *est irréductible, on a* $P = \Pi_{z_1}$ *d'après la question 3b. On en déduit que ses racines complexes sont simples d'après la question 4b.*

► *Soit maintenant* $i \in [\![1, n]\!]$*. Par interpolation de Lagrange, on peut alors trouver* $F \in \mathbb{C}_n[X]$ *tel que* $\forall j \in [\![1, n]\!], F(z_j) = \delta_{i,j}$ *(il y a même un degré « de rab »). En lui appliquant la question précédente, il vient*

$$0 = \sum_{j=1}^{n} F(z_j)(z_j^\ell - z_j^k) = \sum_{j=1}^{n} \delta_{i,j}(z_j^\ell - z_j^k) = z_i^\ell - z_i^k.$$

Ainsi, $z_i^\ell = z_i^k$*, et on obtient l'égalité demandée en divisant par* z_i^k *(de module* 1*, donc non nul).*

Soit $z \in \mathbb{P}_n$*. Le but des questions 13 et 14 est de montrer que* Φ_n *est le polynôme minimal de* z*,* i.e. $\Phi_n = \Pi_z$*. Soit* p *un nombre premier ne divisant pas* n*.*

13. (a) Soient $F, G \in \mathbb{Z}[X]$. Montrer qu'il existe $H \in \mathbb{Z}[X]$ tel que

$$(F + G)^p = F^p + G^p + pH.$$

► *Commençons par montrer que, pour tout* $k \in [\![1, p-1]\!]$*, on a* $p \mid \binom{p}{k}$.

La factorielle $k! = \prod_{j=1}^{k} j$ *est un produit d'entiers non divisibles par* p*, car strictement compris entre* 0 *et* p*, et donc premiers avec le nombre premier* p*. D'après le lemme de Gauss, on en déduit* $p \nmid k!$.

Pour exactement la même raison, $p \nmid (n-k)!$.

Ainsi, l'écriture $(p-1)!\,p = p! = k!\,(n-k)!\binom{p}{k}$ *montre que* $k!\,(n-k)!$ *divise* $(p-1)!\,p$ *tout en étant premier avec* p*. D'après le lemme de Gauss,* $k!\,(n-k)!$ *divise* $(p-1)!$*, donc on peut trouver* $a_{p,k} \in \mathbb{N}$ *tel que* $\binom{p}{k} = p\,a_{p,k}$.

► *Le binôme de Newton et l'argument précédent montrent que*

$$(F+G)^p = F^p + \sum_{k=1}^{p-1} \binom{p}{k} F^k G^{n-k} + G^p$$
$$= F^p + G^p + pH, \qquad \text{où} \quad H = \sum_{k=1}^{p-1} a_{p,k} F^k G^{n-k},$$

ce qui conclut, car ce polynôme H *appartient bien à* $\mathbb{Z}[X]$.

(b) Montrer que $\Pi_z \in \mathbb{Z}[X]$ et en déduire l'existence d'un polynôme $F \in \mathbb{Z}[X]$ tel que

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

► *Le nombre* z *est un entier algébrique en tant que racine de* $X^n - 1$*, donc son polynôme minimal est à coefficients entiers d'après la question 5b.*

► *On écrit* $\Pi_z = \sum_{k=0}^{d} \lambda_k X^k$*, pour certains coefficients* $\lambda_0, \ldots, \lambda_{d-1}, \lambda_d = 1 \in \mathbb{Z}$.
En appliquant de façon répétée la question précédente, on trouve $H \in \mathbb{Z}[X]$ *tel que*

$$\Pi_z^p = \sum_{k=0}^{d} \lambda_k^p X^{p^k} + p\,H.$$

D'après le petit théorème de Fermat, pour tout $k \in [\![0, d]\!]$*, on a* $\lambda_k^p \equiv \lambda_k \pmod{p}$*, ce qui donne l'existence de* $\mu_k \in \mathbb{Z}$ *tel que* $\lambda_k^p = \lambda_k + p\,\mu_k$.
On a donc

$$\Pi_z^p = \sum_{k=0}^{d} (\lambda_k + p\,\mu_k) X^{p^k} + p\,H,$$
$$\text{puis} \quad \Pi_z(X^p) = \sum_{k=0}^{d} \lambda_k X^{p^k}$$
$$= \Pi_z^p + p\,F,$$

où $F = -\left(H + \sum_{k=0}^{d} \mu_k X^{p^k}\right) \in \mathbb{Z}[X]$.

(c) Montrer que $\dfrac{\Pi_z(z^p)}{p}$ est un entier algébrique.

Avec les notations de la question précédente,

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

qui est un entier algébrique en tant que combinaison $\mathbb{Z}$*-linéaire de puissances de* z*, en utilisant à nouveau le fait que les entiers algébriques forment un sous-anneau de* $\mathbb{C}$.

14. (a) Exprimer en fonction de n le nombre $\prod_{1 \leqslant i < j \leqslant n} (z_i - z_j)^2$, où $z_1, z_2, \ldots, z_n$ sont les racines du polynôme $P = X^n - 1$.
Indication : on pourra considérer les nombres $P'(z_i)$.

Le polynôme P *étant unitaire, on a* $P = \prod_{j=1}^{n}(X - z_j)$. *En dérivant,* $P' = \sum_{k=1}^{n} \prod_{\substack{j\in[\![1,n]\!]\\ j\neq k}} (X - z_j)$.

Ainsi, pour tout $i \in [\![1, n]\!]$, *on a*

$$\begin{aligned} P'(z_i) &= \sum_{k=1}^{n} \underbrace{\prod_{\substack{j\in[\![1,n]\!]\\ j\neq k}} (z_i - z_j)}_{=0 \text{ dès que } i \neq k} \\ &= \prod_{\substack{j\in[\![1,n]\!]\\ j\neq i}} (z_i - z_j) \end{aligned}$$

$$\begin{aligned} \textit{donc} \qquad \prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2 &= \prod_{1\leqslant i<j\leqslant n} (z_i - z_j) \times \left[(-1)^{n(n-1)/2} \prod_{1\leqslant j<i\leqslant n} (z_i - z_j) \right] \\ &= (-1)^{n(n-1)/2} \prod_{1\leqslant i\neq j\leqslant n} (z_i - z_j) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(z_i) \\ &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} \left(n\, z_i^{n-1} \right) \\ &= (-1)^{n(n-1)/2}\, n^n \left(\prod_{i=1}^{n} z_i \right)^{-1} \\ &= (-1)^{n(n-1)/2}\, n^n\, (-1)^{n+1} = (-1)^{1+n(n+1)/2}\, n^n, \end{aligned}$$

car $\prod_{i=1}^{n} z_i = (-1)^n \operatorname{coeff}_0(P) = (-1)^{n+1}$.

(b) Montrer que $\Pi_z(z^p) = 0$.
Indication : montrer que si $\Pi_z(z^p) \neq 0$, alors il existe un entier algébrique u tel que $n^n = u \cdot \Pi_z(z^p)$.

- *Commençons par montrer le résultat de l'indication.*
  Comme $P(z) = 0$, *le polynôme unitaire* Π_z *divise* P, *et on peut donc trouver une partie non vide* $J \subseteq [\![1, n]\!]$ *telle que* $\Pi_z = \prod_{j\in J}(X - z_j)$.
  Comme $z^p \in \mathbb{U}_n$, *on peut également trouver* $i_0 \in [\![1, n]\!]$ *tel que* $z^p = z_{i_0}$.
  Si $\Pi_z(z^p)$ *n'était pas nul, on aurait* $i_0 \notin J$, *donc*

$$\begin{aligned} n^n &= \pm \prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2 \\ &= \pm \prod_{j\in J} (z_{i_0} - z_j) \times \prod_{\substack{1\leqslant i<j\leqslant n\\ j\notin J \text{ ou } i\neq i_0}} (z_i - z_j) \times \prod_{1\leqslant i<j\leqslant n} (z_i - z_j) \\ &= \Pi_z(z^p)\, u, \end{aligned}$$

  où $u = \pm \prod_{\substack{1\leqslant i<j\leqslant n\\ j\notin J \text{ ou } i\neq i_0}} (z_i - z_j) \times \prod_{1\leqslant i<j\leqslant n} (z_i - z_j)$ *est encore un entier algébrique d'après le résultat admis dans l'énoncé.*

- *Si $\Pi_z(z^p)$ n'était pas nul, on déduirait du point précédent que $\dfrac{n^n}{p} = u\,\dfrac{\Pi_z(z^p)}{z^p}$ serait un entier algébrique, et donc un entier relatif d'après 5a, ce qui contredit manifestemement le fait que $p \nmid n$.*

(c) Conclure que $\Phi_n = \Pi_z$.

On procède par étapes.

- *Avec les notations de l'énoncé, $\Pi_{z^p} = \Pi_z$, car Π_{z^p} est un polynôme irréductible dont z^p est racine, et la question 3b s'applique.*
- *Par récurrence sur k, on montre que pour toute racine $z \in \mathbb{P}_n$ et tout nombre premier p ne divisant pas n, on a $\forall k \in \mathbb{N}^*, \Pi_{z^{p^k}} = \Pi_z$.*
- *Par récurrence sur le nombre de facteurs premiers de m, on en déduit le résultat plus fort $\forall z \in \mathbb{P}_n, \forall m \in \mathbb{N}, m \perp n \Rightarrow \Pi_{z^m} = \Pi_z$.*
- *Comme les éléments de $\mathbb{P}_n$ sont exactement les z^m, où m décrit l'ensemble des entiers naturels premiers à n, on en déduit*

$$\forall z \in \mathbb{P}_n, \forall \zeta \in \mathbb{P}_n, \Pi_z = \Pi_\zeta,$$

ce qui montre que Π_z possède tous les éléments de $\mathbb{P}_n$ comme racines, et donc qu'il est multiple de Φ_n.
Par irreductibilité, on en déduit $P_z = \Phi_n$.

Partie 3.

Le but de cette partie est d'introduire et d'étudier une certaine classe d'entiers algébriques, qui ne sont pas des racines de l'unité et dont le polynôme minimal possède beaucoup de racines de module 1.

Un polynôme unitaire de degré $d \geqslant 1$

$$P = \sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$$

est dit réciproque *si $a_i = a_{d-i}$ pour $0 \leqslant i \leqslant d$.*

15. (a) Montrer qu'un polynôme $P \in \mathbb{C}[X]$ unitaire de degré d est réciproque si et seulement si $X^d P\left(\dfrac{1}{X}\right) = P$.

C'est une conséquence directe du calcul effectué au début de la question 11c.

(b) Soit $P \in \mathbb{C}[X]$ un polynôme unitaire réciproque. Montrer que si $x \in \mathbb{C}$ est une racine de P, alors $x \neq 0$ et $\dfrac{1}{x}$ est aussi une racine de P, avec la même multiplicité.

- *Soit x une racine de P de multiplicité r. On peut donc trouver $P_0 \in \mathbb{C}[X]$ tel que $P = (X-x)^r P_0$. Comme P est unitaire et réciproque, on a $P(0) = 1$, ce qui prouve que $x \neq 0$.*
- *Par ailleurs, on obtient*

$$\begin{aligned} P = X^{\deg P} P\left(\frac{1}{X}\right) = X^{\deg P}\left(\frac{1}{X} - x\right)^r P_0\left(\frac{1}{X}\right) &= (1-xX)^r X^{\deg P_0} P_0\left(\frac{1}{X}\right) \\ &= (-x)^r \left(X - \frac{1}{x}\right)^r \underbrace{X^{\deg P_0} P_0\left(\frac{1}{X}\right)}_{\in \mathbb{C}[X]}, \end{aligned}$$

ce qui montre que $\dfrac{1}{x}$ est racine de P de multiplicité au moins r.

► *On a donc montré* $\forall x \in \mathbb{C}^*, \mu_{1/x}(P) \geqslant \mu_x(P)$. *En réappliquant cette propriété à* $\dfrac{1}{x}$, *on obtient l'inégalité réciproque, ce qui conclut.*

Si α *est un nombre algébrique de polynôme minimal* Π_α, *les racines complexes de* Π_α différentes de α *sont appelées les* conjugués *de* α. *On notera* $C(\alpha)$ *l'ensemble des conjugués de* α. *L'ensemble* $C(\alpha)$ *est donc vide si* α *est de degré* 1.

16. Soit x un nombre algébrique de module 1 et tel que $x \notin \{-1, 1\}$. Montrer que $\dfrac{1}{x}$ est un conjugué de x. En déduire que Π_x est réciproque.

► *On a* $\dfrac{1}{x} = \overline{x}$ *et* $\Pi_x \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$, *donc* $\dfrac{1}{x}$ *est également racine de* Π_x.

► *Notons* $d = \deg \Pi_x$ *le degré du nombre algébrique* x.

Le polynôme « miroir » $\Pi_x^\dagger = X^d \Pi_x\left(\dfrac{1}{X}\right)$ *possède* x *comme racine d'après ce qui précède, donc* $\Pi_x^\dagger \in I(x)$, *ce qui garantit que le polynôme* Π_x *divise* $\Pi_x^\dagger$.
Comme Π_x *est de degré* d, *le polynôme « miroir »* $\Pi_x^\dagger$ *est non nul, de degré* $\leqslant d$. *La relation de divisibilité que nous avons montrée nous assure donc que* Π_x *et* $\Pi_x^\dagger$ *sont associés : il existe* $u \in \mathbb{C}^*$ *tel que* $\Pi_x^\dagger = u\,\Pi_x$.
Pour déterminer u, *on remarque que la relation* $\Pi_x^\dagger = u\,\Pi_x$ *donne en particulier*

$$1 = \operatorname{coeff}_d(\Pi_x) = \frac{1}{u}\operatorname{coeff}_d(\Pi_x^\dagger) = \frac{1}{u}\operatorname{coeff}_0(\Pi_x) = \frac{1}{u^2}\operatorname{coeff}_0(\Pi_x^\dagger) = \frac{1}{u^2}\operatorname{coeff}_d(\Pi_x) = \frac{1}{u^2},$$

ce qui montre $u = \pm 1$.
Enfin, si u *valait* -1, *on aurait* $\forall i \in [\![0, d]\!], a_{d-i} = -a_i$, *ce qui entraîne que la somme des coefficients de* Π_x *vaut* 0 *et donc que* $\Pi_x(1) = 0$. *C'est impossible : l'irréductibilité de* Π_x *entraînerait* $\Pi_x = X - 1$ *et donc* $x = 1$, *ce qui a été exclu.*
On en déduit que $u = 1$, *et donc que* Π_x *est réciproque.*

On note $\mathcal{S}$ *l'ensemble des nombres réels* $\alpha \in]1, +\infty[$ *qui sont aussi des entiers algébriques de degré au moins* 2 *et qui vérifient*

$$\max_{\gamma \in C(\alpha)} |\gamma| = 1.$$

17. Soit α un élément de $\mathcal{S}$ et soit $\gamma \in C(\alpha)$ de module 1.

(a) Montrer que le polynôme minimal de α est réciproque et que $\dfrac{1}{\alpha}$ est un conjugué de α.

► *Le polynôme* Π_α *est irréductible (d'après la question 3a) et annule* γ, *donc* $\Pi_\alpha = \Pi_\gamma$ *d'après la question 3b.*

► *En particulier,* γ *est de même degré que* α, *donc de degré* > 1, *d'où* $\gamma \notin \{-1, 1\}$.

► *La question 16 entraîne donc que* $\Pi_\alpha = \Pi_\gamma$ *est réciproque et la question 15b entraîne que* $\dfrac{1}{\alpha} \in]0, 1[$ *est une racine de* Π_α. *Comme* $\dfrac{1}{\alpha} \neq \alpha$, *cela dit bien que* $\dfrac{1}{\alpha}$ *est conjugué à* α.

(b) Montrer que γ n'est pas une racine de l'unité.

Si γ *était une racine de l'unité, on aurait* $\Pi_\gamma = \Phi_d$ *pour un certain entier* d *(d'après la partie 2), puis* $\Pi_\alpha = \Pi_\gamma = \Phi_d$, *ce qui est aburde, car* α *appartient à* $]1, +\infty[$, *qui est disjoint de* Π_d *: il ne saurait donc être racine de* Φ_d.

(c) Montrer que tous les conjugués de α autres que $\dfrac{1}{\alpha}$ sont de module 1.

Soit $\beta \in C(\alpha)$ de module $\neq 1$. On va montrer $\beta = \dfrac{1}{\alpha}$.
Déjà, comme $\alpha \in \mathcal{S}$, on a $|\beta| \leqslant |\gamma| = 1$, donc $|\beta| < 1$.
Comme Π_α est réciproque, on sait que $\dfrac{1}{\beta}$ est aussi racine de Π_α. Puisque $\left|\dfrac{1}{\beta}\right| > 1$, cette racine ne peut pourtant pas appartenir à $C(\alpha)$.
On doit donc avoir $\dfrac{1}{\beta} = \alpha$, d'où il vient $\beta = \dfrac{1}{\alpha}$.

18. Montrer que le degré de tout élément de $\mathcal{S}$ est un entier pair, supérieur ou égal à 4.

Notons $D = C(\alpha) \cup \{\alpha\}$ (union trivialement disjointe), qui est l'ensemble des racines de Π_α.

- *Comme toutes les racines de Π_α sont simples (question 4b), on a $|D| = \deg \Pi_\alpha$, qui est le degré de α.*
- *Comme à la question 17a, on a que pour tout $\delta \in D$, $\deg \Pi_\delta = \deg \Pi_\alpha > 1$.*
  Notamment, $D \cap \{-1, 1\} = \varnothing$.
- *Puisque Π_α est réciproque, l'ensemble D est inclus dans $\mathbb{C}^*$ et stable sous l'application $i : x \mapsto -x$. L'application i est donc une involution de D, et elle ne possède pas de point fixe d'après le point précédent.*
  Cela montre que D est une union disjointe de paires $\left\{\delta, \dfrac{1}{\delta}\right\}$ et donc que $|D|$ est un entier pair.
- *Enfin, D doit au moins contenir $\dfrac{1}{\alpha} \in]0, 1[$, $\gamma \in \mathbb{U}$ et $\alpha \in]1, +\infty[$, distincts, donc $|D| \geqslant 3$.*

On en déduit que $|D|$ est un entier pair $\geqslant 4$.

Partie 4.

Dans cette partie, on étudie une famille infinie d'éléments de l'ensemble $\mathcal{S}$ introduit dans la partie 3, avant la question 17.

Pour tout entier $n > 1$, on définit $P_n \in \mathbb{Z}[X]$ par

$$P_n = X^4 - (6+n)X^3 + (10+n)X^2 - (6+n)X + 1.$$

19. Vérifier que P_n n'a pas de racine dans $\mathbb{Q}$ et que P_n a au moins une racine réelle strictement plus grande que 1. On fixe une telle racine α_n dans la suite.

D'après la question 5a, une éventuelle racine rationnelle z serait nécessairement entière. L'égalité $P_n(z) = 0$ se réécrirait alors

$$z\big(\underbrace{-z^3 + (6+n)z^2 - (10+n)z + (6+n)}_{\in\mathbb{Z}}\big) = 1,$$

ce qui montre que $z = \pm 1$.
Or, on a $P_n(-1) = 24 + 3n > 0$ et $P_n(1) = -n < 0$, ce qui montre que 1 et -1 ne sont pas racines de P_n. Ce polynôme n'a donc pas de racine rationnelle.
Par ailleurs, la fonction polynomiale $t \mapsto P_n(t)$ est continue, strictement négative en 1 et diverge vers $+\infty$ en $+\infty$, donc le théorème des valeurs intermédiaires entraîne qu'elle s'annule au moins une fois sur l'intervalle $]1, +\infty[$.

20. Montrer que si $x \in \mathbb{C}$ est une racine de P_n, alors $\dfrac{1}{x}$ est aussi une racine de P_n, avec la même multiplicité.

Il suffit de remarquer que P_n est unitaire et réciproque, et d'appliquer la question 15b.

On note α_n, $\dfrac{1}{\alpha_n}$, γ_n, $\dfrac{1}{\gamma_n}$ *les racines de* P_n *dans* $\mathbb{C}$ *et on pose*

$$t_n = \alpha_n + \frac{1}{\alpha_n}, \qquad s_n = \gamma_n + \frac{1}{\gamma_n}.$$

21. Montrer que $t_n + s_n = 6 + n$ et $t_n s_n = 8 + n$.

- *Puisque les racines (toutes simples) de* P_n *sont* α_n, $\dfrac{1}{\alpha_n}$, γ_n *et* $\dfrac{1}{\gamma_n}$, *la somme* $t_n + s_n$ *est la somme des racines de* P_n, *donc* $t_n + s_n = -\operatorname{coeff}_3(P_n) = 6 + n$.
- *En développant, on voit que* $t_n\, s_n$ *est la somme des produits de deux racines de* P_n, *à l'exception des deux produits* $\alpha_n \dfrac{1}{\alpha_n} = \gamma_n \dfrac{1}{\gamma_n} = 1$. *On a donc, d'après les relations de Viète,*

$$t_n\, s_n = \operatorname{coeff}_2(P_n) - 2 = (10 + n) - 2 = 8 + n.$$

22. Montrer que s_n est réel et que $0 < s_n < 2$. En déduire que γ_n n'est pas réel et que γ_n est de module 1.

Les nombres t_n *et* s_n *sont les racines du polynôme* $X^2 - (6+n)X + 8 + n$, *d'après la question précédente.*

- *Ce polynôme possède déjà une racine réelle, à savoir* $t_n = \alpha_n + \dfrac{1}{\alpha_n} \in]2, +\infty[$.
- *Par ailleurs, ce polynôme vaut* $8 + n > 0$ *en* 0 *et* $-n < 0$ *en* 2, *donc il possède une racine dans* $]0, 2[$. *Il ne peut s'agir que de* s_n.
- *Si* γ_n *était réel, une étude rapide de la fonction* $x \mapsto x + \dfrac{1}{x}$ *(à vrai dire déjà utilisée dans le premier point) montre que l'on aurait* $s_n \leqslant -2$ *ou* $s_n \geqslant 2$, *suivant le signe de* γ_n. *On a donc* $\gamma_n \notin \mathbb{R}$.
- *Puisque* $\gamma_n \notin \mathbb{R}$, *son conjugué* $\overline{\gamma}_n \neq \gamma_n$ *est une autre racine non réelle du polynôme* P_n, *ce qui montre* $\overline{\gamma}_n = \dfrac{1}{\gamma_n}$ *et donc* $|\gamma_n| = 1$.

23. (a) Montrer que t_n et s_n sont irrationnels.

Les nombres t_n *et* s_n *sont les racines de* $Q = X^2 - (6 + n)X + 8 + n \in \mathbb{Z}[X]$.

- *D'après 5a, s'ils étaient rationnels, ils seraient entiers.*
- *En notant* Δ *le discriminant de* Q, *on aurait donc* $\dfrac{6 + n \pm \sqrt{\Delta}}{2} \in \mathbb{Z}$, *ce qui entraîne directement que* $\sqrt{\Delta} \in \mathbb{Z}$ *: le discriminant* Δ *serait un carré parfait.*
  Or, $\Delta = (6 + n)^2 - 4(8 + n) = n^2 + 8n + 4$.
  - *Si* $n = 2$, $\Delta = 24$ *n'est pas un carré parfait.*
  - *Si* $n \geqslant 3$, *on a* $2n - 5 > 0$, *ce qui donne l'encadrement strict*

$$(n + 3)^2 = n^2 + 6n + 9 < n^2 + 8n + 4 < n^2 + 8n + 16 = (n + 4)^2,$$

  et montre que $n^2 + 8n + 4$ *n'est pas un carré parfait.*

Cela conclut.

(b) En déduire que P_n est irréductible dans $\mathbb{Q}[X]$ et que $\alpha_n \in \mathcal{S}$.

- *Supposons par l'absurde pouvoir trouver deux polynômes non constants* $Q, R \in \mathbb{Q}[X]$ *tels que* $P_n = QR$.
  - *Quitte à multiplier* Q *et* R *par* λ *et* $\dfrac{1}{\lambda}$, *où* λ *est le coefficient dominant de* R, *on peut supposer* Q *et* R *unitaires.*

- *Comme* P_n *n'a pas de racine rationnelle, on a nécessairement* $\deg Q, \deg R > 1$, *c'est-à-dire* $\deg Q = \deg R = 2$.
- *Le nombre complexe* γ_n *est racine de l'un des deux facteurs, disons* Q.

  Comme Q *est réel, on a nécessairement que* $\overline{\gamma}_n = \dfrac{1}{\gamma_n}$ *est sa seconde racine, donc on a* $Q = (X-\gamma_n)(X-\overline{\gamma}_n) = X^2 - s_n X + 1$.

  Or, $s_n \notin \mathbb{Q}$, *donc* $Q \notin \mathbb{Q}[X]$, *ce qui fournit la contradiction souhaitée.*

Cela montre que P_n *est irréductible dans* $\mathbb{Q}[X]$.

► *Ce qui précède montre que* $P_n = \Pi_{\alpha_n}$.

- *Racine d'un polynôme unitaire à coefficients entiers,* α_n *est un entier algébrique, de degré* 4.
- *On a* $C(\alpha_n) = \left\{\dfrac{1}{\alpha_n}, \gamma_n, \overline{\gamma}_n\right\}$, *donc* $\alpha_n \in \mathcal{S}$.

(c) Montrer que $\lim\limits_{n\to+\infty} \alpha_n = +\infty$.

► *On a* $s_n \leqslant 2$, *donc* $t_n \geqslant (s_n + t_n) - 2 = 4 + n$.

► *On a* $\dfrac{1}{\alpha_n} \in]0,1[$, *donc* $\alpha_n \geqslant t_n - 1 = 3 + n$.

Cela montre $\alpha_n \xrightarrow[n\to+\infty]{} +\infty$, *par minoration.*

24. Soit $\mathcal{T}$ l'ensemble des $\alpha \in \mathcal{S}$ de degré 4. Montrer que $\mathcal{T}$ possède un plus petit élément et calculer ce nombre.

D'après la partie 3, le polynôme minimal d'un $\alpha \in \mathcal{T}$ *est* $\Pi_\alpha = (X-\alpha)\left(X - \dfrac{1}{\alpha}\right)(X-\gamma)(X-\overline{\gamma})$, *où* $\gamma \in \mathbb{U}$. *Si l'on note* $t = \alpha + \dfrac{1}{\alpha} \in]2,+\infty[$ *et* $s = \gamma + \overline{\gamma} = 2\,\mathrm{Ré}\,\gamma \in]-2,2[$, *on a également* $\Pi_\alpha = (X^2 - tX + 1)(X^2 - sX + 1) = (X^4 - aX^3 + bX^2 - aX + 1)$, *où* $a = t + s$ *et* $b = 2 + ts$.
En particulier, s *et* t *sont racines du polynôme* $Q = X^2 - (t+s)X + ts = X^2 - aX + b - 2 \in \mathbb{Z}[X]$.
Cela montre déjà qu'ils sont entiers algébriques, de degré $\leqslant 2$, *et on peut même voir que leur degré est exactement* 2 *:*

► *si* t *était de degré* 1, *il serait rationnel, et* α, *qui est racine de* $X^2 - tX + 1$ *ne pourrait pas alors être de degré* 4 *;*

► *d'après la relation* $s + t = a$, *si* s *était rationnel,* t *le serait aussi, ce qui est exclu (je n'utilise pas directement ce fait dans la suite, mais je n'allais pas casser la symétrie entre* s *et* t*).*

Par ailleurs, $a = s + t > 0$ *car* $s \in]-2,2[$ *et* $t \in]2,+\infty[$, *donc* $a \in \mathbb{N}^*$.
La fonction $x \mapsto x + \dfrac{1}{x}$ *étant strictement croissante sur* $]1,+\infty[$, *il revient au même de minimiser* α *et de minimiser* t. *Comme* t *est la plus grande racine des deux racines (qui sont réelles) de* Q, *on obtient directement que* $b < \dfrac{a^2}{4} + 2$ *et que*

$$t = \frac{a + \sqrt{a^2 - 4b + 8}}{2}.$$

Notons déjà que cela entraîne trivialement $t \geqslant \dfrac{a}{2}$.

Le cas $a = 1$ *et* $b = -1$ *donne* $t_0 = \dfrac{1+\sqrt{13}}{2}$, *dont nous allons voir qu'il est le plus petit possible, plus ou moins par exhaustion des cas.*

► *Si* $a = 1$, *toute valeur* $b < -1$ *donnera* $t > \dfrac{1+\sqrt{13}}{2}$, *donc on examine les valeurs positives de* b *:*

- $b = 0$ *donne* $t = 2$, *qui n'est pas un entier algébrique de degré* 2 ;
- $b = 1$ *donne* $t = \dfrac{1+\sqrt{5}}{2}$, *qui est* < 2 *et est donc exclu.* A fortiori, *toute valeur supérieure de* b *donnera un résultat encore plus petit (jusqu'à ce que* $a^2 - 4b + 8$ *devienne* < 0, *ce qui est encore plus exclu).*

▸ *Si* $a = 2$, *on doit avoir* $b < \dfrac{a^2}{4} + 2 = 3$:

- $b = 2$ *donne* $t = 2$, *qui n'est pas un entier algébrique de degré* 2 ;
- $b = 1$ *donne* $t = 1 + \sqrt{2}$, *dont on vérifie qu'il est* $> t_0$:

$$1 + \sqrt{2} > \frac{1+\sqrt{13}}{2} \Leftrightarrow 1 + 2\sqrt{2} > \sqrt{13} \Leftrightarrow 9 + 4\sqrt{2} > 13 \Leftrightarrow 4\sqrt{2} > 4,$$

ce qui est évidemment vrai. Les valeurs $b < 1$ *donneront des résultats encore plus grands, que nous n'avons pas besoin d'examiner.*

▸ *Si* $a = 3$, *on doit avoir* $b < \dfrac{9}{4} + 2$, *c'est-à-dire* $b \leqslant 4$:

- $b = 4$ *donne* $t = 1$, *exclu ;*
- $b = 3$ *donne* $t = \dfrac{3+\sqrt{5}}{2}$, *dont on montre comme dans le cas* $a = 2, b = 1$, *qu'il est* $> t_0$, *ce qui nous dispense d'examiner les cas suivants.*

▸ *Si* $a = 4$, *on doit avoir* $b < 6$:

- $a = 5$ *donne* $t = 3$, *ce qui est exclu pour des raisons de degré, mais qui est aussi* $> t_0$, *ce qui nous dispense d'examiner les cas suivants.*

▸ *Si* $a \geqslant 5$, *on a* $a > 1 + \sqrt{13}$, *donc* $t \geqslant \dfrac{a}{2} > t_0$, *et ces cas sont exclus.*

In fine, *quel que soit* $\alpha \in \mathcal{T}$, *on aura* $t \geqslant \dfrac{1+\sqrt{13}}{2}$, *ce cas correspondant à la situation où* α *est la plus grande racine réelle de* $(a = 1, b = -1)$

$$P = X^4 - X^3 - X^2 - X + 1 = \left(X^2 - \frac{1+\sqrt{13}}{2}X + 1\right)\left(X^2 - \frac{1-\sqrt{13}}{2}X + 1\right),$$

c'est-à-dire (après calcul) $\alpha = \dfrac{1}{4}\left(1 + \sqrt{13} + \sqrt{2\sqrt{13} - 2}\right)$.

Ce nombre est bien élément de $\mathcal{T}$: *les nombres* $\dfrac{1 \pm \sqrt{13}}{2}$ *sont irrationnels et l'on peut suivre le raisonnement de la question 23b pour en déduire que* P *est irréductible, ce qui montre* $P = \Pi_\alpha$ *et donc que* α *est un entier algébrique de degré* 4, *dont les conjugués sont* $\dfrac{1}{\alpha}$ *et les deux racines de* $X^2 - \dfrac{1-\sqrt{13}}{2}X + 1$, *qui sont non réelles (par un simple calcul de discriminant) donc s'écrivent* γ *et* $\overline{\gamma}$, *et vérifient* $|\gamma|^2 = \gamma\,\overline{\gamma} = 1$ *d'après les relations de Viète.*

On ne sait pas si l'ensemble $\mathcal{S}$ *possède un plus petit élément. Le plus petit élément de* $\mathcal{S}$ *connu est la plus grande racine réelle du polynôme* $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$.