DM 20 : polynômes cyclotomiques et nombres de Salem

Ce problème est un sujet de concours (concours commun X-ÉNS 2019, maths A) à peine modifié.

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 $\mathrm{coeff}_k(F) = \dfrac{F^{(k)}(0)}{k!}$.

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 $\{0\}$.

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 $\alpha \in \mathbb{Q}$.
3. (a) Montrer que Π_α est irréductible dans $\mathbb{Q}[X]$.
   (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.
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 $\mathbb{Q}[X]$.
   (b) Montrer que les racines de Π_α dans $\mathbb{C}$ sont simples.
5. (a) Montrer que si $\alpha \in \mathbb{Q}$ est un entier algébrique, alors $\alpha \in \mathbb{Z}$.
   (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.
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.
   (b) Montrer que $\frac{3+4i}{5}$ est un nombre algébrique de degré 2 et de module 1 mais n'est pas une racine de l'unité.

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.

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

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

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

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

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

(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.

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

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 $\mathcal{E}_{\mathbb{Z}} = \{F \in \mathcal{E} \mid \forall k \in \mathbb{N}, \text{coeff}_k(F) \in \mathbb{Z}\}$.
    (a) Montrer que $\mathcal{E}$ et $\mathcal{E}_{\mathbb{Z}}$ sont des sous-anneaux de $\mathbb{C}(X)$.
    (b) Soit $D \in \mathbb{Z}[X]$ tel que $D(0) = 1$. Montrer que D est un élément inversible de $\mathcal{E}_{\mathbb{Z}}$.
    (c) Montrer que $X^n P\left(\frac{1}{X}\right)$ est un élément inversible de $\mathcal{E}_{\mathbb{Z}}$ et en déduire l'existence de $F \in \mathcal{E}_{\mathbb{Z}}$ telle que
    $$X F(X) P\left(\frac{1}{X}\right) = P'\left(\frac{1}{X}\right).$$
    (d) Obtenir une expression explicite de F sous forme d'une somme finie et en déduire que $\forall k \in \mathbb{Z}, a_k \in \mathbb{Z}$.
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.
    (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.
    (c) Montrer que $z_1, z_2, \ldots, z_n$ sont deux à deux distincts. En déduire que $z_i^{\ell-k} = 1$ pour tout $i \in \{1, 2, \ldots, n\}$ et conclure.

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
    $$(F + G)^p = F^p + G^p + pH.$$
    (b) Montrer que $\Pi_z \in \mathbb{Z}[X]$ et en déduire l'existence d'un polynôme $F \in \mathbb{Z}[X]$ tel que
    $$\Pi_z(X^p) = \Pi_z(X)^p + pF(X).$$
    (c) Montrer que $\dfrac{\Pi_z(z^p)}{p}$ est un entier algébrique.
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 $P'(z_i)$.
    (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 $n^n = u \cdot \Pi_z(z^p)$.
    (c) Conclure que $\Phi_n = \Pi_z$.

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 $X^d P\left(\frac{1}{X}\right) = P$.

    (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 $\frac{1}{x}$ est aussi une racine de P, avec la même multiplicité.

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 $\frac{1}{x}$ est un conjugué de x. En déduire 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 $\frac{1}{\alpha}$ est un conjugué de α.

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

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

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

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 $t_n s_n = 8 + n$.
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.
23. (a) Montrer que t_n et s_n sont irrationnels.
    (b) En déduire que P_n est irréductible dans $\mathbb{Q}[X]$ et que $\alpha_n \in \mathcal{S}$.
    (c) Montrer que $\lim\limits_{n\to+\infty} \alpha_n = +\infty$.
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.

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 $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$.