Devoir maison n° 5

(à rendre le mercredi 22 novembre 2023)

Notations. 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 $P \in \mathbb{Z}[X]$, irréductibles dans $\mathbb{Q}[X]$ et qui possèdent beaucoup de racines de module 1.

Première partie

Dans les questions 1 à 3, on fixe un nombre algébrique α. On pose : $I(\alpha) = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$. On a vu en cours qu'il existe un unique polynôme unitaire $\pi_\alpha \in \mathbb{Q}[X]$, 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.

Le but de cette partie est de montrer que le polynôme minimal d'un entier algébrique est dans $\mathbb{Z}[X]$.

1. Montrer que α est de degré 1 si et seulement si : $\alpha \in \mathbb{Q}$.
2. (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.
3. (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.
4. (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 4.(a).
5. (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.

Deuxième partie

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.

Soit $n \in \mathbb{N}\backslash\{0\}$. On dit qu'une racine n^{e} de l'unité z est primitive si $z^d \neq 1$ pour tout entier d tel que $1 \leqslant d < n$. On note μ_n l'ensemble des racines primitives n^{es} de l'unité. On a donc : $\mu_1 = \{1\}$. On définit $\Phi_n \in \mathbb{C}[X]$ par : $\Phi_n = \prod_{z \in \mu_n} (X - z)$.

6. Montrer que pour tout $n \in \mathbb{N} \setminus \{0\}$, on a : $X^n - 1 = \prod_{d|n} \Phi_d$, le produit étant sur les diviseurs *positifs* de n.
7. (a) Montrer que si p est un nombre premier et $k \geqslant 1$ un entier, alors : $\Phi_{p^k} = \sum_{j=0}^{p-1} X^{jp^{k-1}}$.
   (b) Calculer Φ_n pour tout $n \in [\![1,6]\!]$.

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

8. (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 6.

9. Montrer : $\Phi_n \in \mathbb{Z}[X]$.

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 10 et 11 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 :

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

10. (a) Montrer que la série $\sum_{k \geqslant 0} a_k z^k$ converge pour tout $z \in \mathbb{C}$ tel que : $|z| < 1$.
    (b) Soit $z \in \mathbb{C}^*$ tel que $|z| < 1$ et soit $f(z) = \sum_{k=0}^{+\infty} a_k z^k$. Montrer : $z f(z) P\left(\frac{1}{z}\right) = P'\left(\frac{1}{z}\right)$.
    (c) En déduire que $a_k \in \mathbb{Z}$ pour tout $k \in \mathbb{N}$. *Indication : utiliser l'unicité de la partie régulière d'un développement limité, ou pour les cinq-demis : la théorie des séries entières.*
11. (a) Montrer qu'il existe deux entiers $0 \leqslant k < \ell$ tels que $a_{k+i} = a_{\ell+i}$ pour tout $i \in [\![0, n]\!]$.
    On fixe deux tels entiers k, ℓ dans les questions 11.(b) et 11.(c).
    (b) Montrer que $\sum_{i=1}^{n} F(z_i)\left(z_i^{\ell} - z_i^{k}\right) = 0$ pour tout $F \in \mathbb{C}[X]$ de degré inférieur ou égal à n.
    (c) Montrer que $z_1, z_2, \ldots, z_n$ sont deux à deux distincts. En déduire : $\forall i \in [\![1, n]\!]$, $z_i^{\ell-k} = 1$, et conclure.

Soit $z \in \mu_n$. Le but des questions 12 et 13 est de montrer que Φ_n est le polynôme minimal de z, c'est-à-dire : $\Phi_n = \pi_z$. Soit p un nombre premier ne divisant pas n.

12. (a) Soit $(F, G) \in (\mathbb{Z}[X])^2$. Montrer qu'il existe $H \in \mathbb{Z}[X]$ tel que : $(F+G)^p = F^p + G^p + pH$.
    (b) Montrer : $\pi_z \in \mathbb{Z}[X]$, et en déduire l'existence $F \in \mathbb{Z}[X]$ tel que : $\pi_z(X^p) = \pi_z(X)^p + pF(X)$.
    (c) Montrer que $\frac{\pi_z(z^p)}{p}$ est un entier algébrique.
13. (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 : $\pi_z(z^p) = 0$. *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 : $\Phi_n = \pi_z$.

Troisième partie

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 $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$ unitaire de degré $d \geqslant 1$ est dit *réciproque* si : $\forall i \in [\![0, d]\!]$, $a_i = a_{d-i}$.

14. (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.

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

16. 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.
17. Montrer que le degré de tout élément de $\mathcal{S}$ est un entier pair, supérieur ou égal à 4.