DM02 - A rendre lundi 09/10/2023

Nombres algébriques et entiers algébriques

Notations

On notera respectivement $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ les corps des nombres complexes, réels et rationnels, et $\mathbb{Z}$ l'anneau des entiers relatifs.
Pour un entier $n \geq 1$, 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 $k \geq 1$ 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.
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 1
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.

Partie I

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*

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

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

Il existe donc un unique polynôme unitaire $\Pi_\alpha \in \mathbb{Q}[X]$, appelé polynôme minimal de α, tel que

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

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 5.(a).
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 II

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 $d \geq 1$

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

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

7. (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.

8. 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*

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

9. 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.
10. Montrer que le degré de tout élément de $\mathcal{S}$ est un entier pair, supérieur ou égal à 4.