

DS 6 de mathématiques

Durée : 4h.

- Les calculatrices et autres technologies sont interdites.
- Une attention particulière sera portée à la qualité de la rédaction et à la rigueur du raisonnement. La copie doit être lisible, les pages numérotées, les calculs suffisamment détaillés, les résultats mis en valeur...
- Les trois problèmes sont indépendants et peuvent être traités dans un ordre quelconque.
- Si vous repérez une possible erreur d'énoncé, vous êtes invité(e) à venir le signaler.

1 Entiers algébriques

Définitions et résultats admis

On rappelle les définitions et résultats suivants, vus en DM ou TD.

- Un nombre complexe α est algébrique s'il existe $P \in \mathbb{Q}[X]$ non nul tel que $P(\alpha) = 0$.
- Si α est algébrique, il existe un unique $P_\alpha \in \mathbb{Q}[X]$ unitaire tel que :

$$\forall Q \in \mathbb{Q}[X], Q(\alpha) = 0 \iff P_\alpha \mid Q.$$

On dit que P_α est le polynôme minimal de α . C'est un polynôme irréductible dans $\mathbb{Q}[X]$ et on appelle degré de α le degré de P_α .

- On note $\mathbb{Z}[X]$ le sous-anneau de $\mathbb{Q}[X]$ constitué des polynômes à coefficients entiers.
- Si $P \in \mathbb{Z}[X]$, on note $c(P)$ le contenu de P , défini comme le pgcd des coefficients de P . Pour tous $P, Q \in \mathbb{Z}[X]$, on a $c(PQ) = c(P)c(Q)$.

1.1 Généralités

Un nombre complexe α est un entier algébrique s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$. Un tel nombre est en particulier un nombre algébrique.

1. Montrer que $\sqrt[3]{2}$ et $e^{i\pi/3}$ sont des entiers algébriques. Déterminer leur polynôme minimal.
2. Montrer que $\sqrt{2} + i$ est un entier algébrique. Déterminer son polynôme minimal.
3. Montrer que α est un entier algébrique ssi $P_\alpha \in \mathbb{Z}[X]$.
On utilisera le résultat admis sur les contenus de polynômes de $\mathbb{Z}[X]$.
4. Montrer que $\omega = \frac{3+4i}{5}$ est un élément de $\mathbb{U}$, mais que ce n'est pas une racine de l'unité.

Soit $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$ un polynôme unitaire de degré $d \geq 1$ de racines $\alpha_1, \dots, \alpha_d$, répétées selon leur multiplicité. On note

- $\mathcal{M}(P) = \prod_{i=1}^d \max(1, |\alpha_i|)$ la mesure de Mahler de P ;
- $h(P) = \max_{0 \leq k \leq d} |a_k|$ la hauteur de P .

5. Pour tout $k \in \llbracket 0, d-1 \rrbracket$, rappeler l'expression de a_k en fonction de $\alpha_1, \dots, \alpha_d$.

6. Montrer que pour tout $i \in \llbracket 0, d \rrbracket$, $\binom{d}{i} \leq 2^{d-1}$.

7. En déduire que $\mathcal{M}(P) \geq \frac{h(P)}{2^{d-1}}$.

Pour tout $n \in \mathbb{N}$ et pour tout $A \in \mathbb{R}_+^*$, on désigne par $\mathcal{P}_{n,A}$ l'ensemble :

$$\mathcal{P}_{n,A} = \{P \in \mathbb{Z}[X] \cap \mathbb{Q}_n[X] \mid P \text{ unitaire et } \mathcal{M}(P) \leq A\}.$$

8. Montrer que $\mathcal{P}_{n,A}$ est fini.

1.2 Théorème de Kronecker

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré d , de racines complexes $\alpha_1, \dots, \alpha_d$.

9. Montrer qu'il existe un unique couple $(F, G) \in \mathbb{Z}[X]^2$ tel que $P = F(X^2) + XG(X^2)$.

10. Montrer que $F^2 - XG^2 = (-1)^d \prod_{i=1}^d (X - \alpha_i^2)$.

Si α est un entier algébrique, on appelle conjugués de α les racines complexes de P_α (on inclut α dans cette définition).

11. Soit $n \in \mathbb{N}^*$. On considère $\alpha \in \mathbb{C}$ un entier algébrique de degré inférieur à n .

(a) Montrer que α^2 est aussi un entier algébrique de degré inférieur à n .

On suppose de plus que les conjugués β de α vérifient $|\beta| \leq 1$.

(b) Montrer que les conjugués de α^2 vérifient la même propriété.

12. Soit α un entier algébrique non nul dont les conjugués β vérifient $|\beta| \leq 1$.
Montrer¹ que α est une racine de l'unité.

¹Théorème dû au mathématicien allemand Leopold Kronecker (1823 – 1891), démontré en 1857.

1.3 Nombres de Pisot-Vijayaraghavan

Un nombre réel $\alpha > 1$ est un nombre de Pisot²-Vijayaraghavan³ (abrégé nombre PV) si c'est un entier algébrique et si tous les conjugués β de α , distincts de α , vérifient $|\beta| < 1$.

13. Montrer qu'il existe un unique réel ψ vérifiant $\psi^3 = \psi + 1$ et qu'il vérifie $\psi > 1$.
14. Montrer que ψ est un nombre PV de degré 3.

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $d \geq 1$, de racines $\alpha_1, \dots, \alpha_d$. On note

- $S_p = \sum_{i=1}^d \alpha_i^p$, pour tout $p \in \mathbb{N}$;
- $\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq d} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}$, pour tout $k \in \llbracket 1, d \rrbracket$.

15. Soit $i \in \llbracket 1, d \rrbracket$. Montrer que $\alpha_i^d - \sigma_1 \alpha_i^{d-1} + \dots + (-1)^{d-1} \sigma_{d-1} \alpha_i + (-1)^d \sigma_d = 0$.
16. En déduire que, pour tout $p \geq d$,

$$S_p - \sigma_1 S_{p-1} + \dots + (-1)^{d-1} \sigma_{d-1} S_{p-d+1} + (-1)^d \sigma_d S_{p-d} = 0.$$

On admet que, pour tout $p \leq d-1$, on a la relation :

$$S_p - \sigma_1 S_{p-1} + \dots + (-1)^{p-1} \sigma_{p-1} S_1 + (-1)^p p \sigma_p = 0.$$

17. Montrer que, pour tout $p \in \mathbb{N}$, $S_p \in \mathbb{Z}$.

Pour tout $x \in \mathbb{R}$, on note $d(x, \mathbb{Z}) = \min \{|x - k|, k \in \mathbb{Z}\}$.

18. Montrer que si α est un nombre PV, alors $d(\alpha^n, \mathbb{Z}) \rightarrow 0$, quand $n \rightarrow +\infty$.

²D'après Charles Pisot (1910 – 1984), mathématicien français

³D'après Tirukkannapuram Vijayaraghavan (1902 – 1955), mathématicien indien

2 Automorphismes d'algèbre de $\mathcal{L}(E)$

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$.

Une application $\phi : \mathcal{L}(E) \rightarrow \mathcal{L}(E)$ est un automorphisme d'algèbre de $\mathcal{L}(E)$ si c'est un automorphisme, pour les structures de $\mathbb{K}$ -espace vectoriel et d'anneau de $\mathcal{L}(E)$; autrement dit, si c'est un élément $\phi \in \text{GL}(\mathcal{L}(E))$ tel que $\phi(\text{id}_E) = \text{id}_E$ et $\phi(g \circ f) = \phi(g) \circ \phi(f)$, pour tous $f, g \in \mathcal{L}(E)$.

On désigne par $\mathcal{A}$ l'ensemble de ces automorphismes d'algèbre.

1. Montrer que $(\mathcal{A}, \circ)$ est un groupe.
2. Soit $u \in \text{GL}(E)$. On note ϕ_u l'application définie de $\mathcal{L}(E)$ dans $\mathcal{L}(E)$ par

$$\forall f \in \mathcal{L}(E), \phi_u(f) = u^{-1} \circ f \circ u.$$

Montrer que $\phi_u \in \mathcal{A}$.

Soit $\phi \in \mathcal{A}$. On fixe une base $(e_1, \dots, e_n)$ de E . Pour tout $k \in \llbracket 1, n \rrbracket$, on note $D_k = \text{Vect}(e_k)$ et p_k le projecteur sur D_k parallèlement à $\bigoplus_{i \neq k} D_i$.

3. Montrer que, pour tout $k \in \llbracket 1, n \rrbracket$, $\phi(p_k)$ est un projecteur non nul de $\mathcal{L}(E)$.
4. Pour tout $k \in \llbracket 1, n \rrbracket$, on note $F_k = \text{Im}(\phi(p_k))$. Montrer que les F_k sont en somme directe dans E . En déduire leur dimension, puis que $E = \bigoplus_{k=1}^n F_k$.
5. Pour tout $k \in \llbracket 1, n \rrbracket$, on fixe un vecteur non nul f_k dans F_k .
Montrer qu'il existe $u \in \text{GL}(E)$ tel que $\forall k \in \llbracket 1, n \rrbracket, u(e_k) = f_k$.
6. On note $\psi = \phi_u \circ \phi$. Montrer que, pour tout $k \in \llbracket 1, n \rrbracket$, $\psi(p_k) = p_k$.

Pour tous $i, j \in \llbracket 1, n \rrbracket$, on note $f_{i,j}$ l'unique endomorphisme de E tel que $f_{i,j}(e_i) = e_j$ et $f_{i,j}(e_k) = 0$ si $k \in \llbracket 1, n \rrbracket \setminus \{i\}$. On remarque que $f_{i,i} = p_i$, pour tout $i \in \llbracket 1, n \rrbracket$.

7. Montrer que la famille $(f_{i,j})_{(i,j) \in \llbracket 1, n \rrbracket^2}$ est une base de $\mathcal{L}(E)$.
8. Calculer, pour tous $i \neq j \in \llbracket 1, n \rrbracket$, $p_j \circ f_{i,j}$ et $f_{i,j} \circ p_i$.
9. En déduire que, pour tous $i, j \in \llbracket 1, n \rrbracket$, il existe $\alpha_{i,j} \in \mathbb{K}^*$ tel que $\psi(f_{i,j}) = \alpha_{i,j} f_{i,j}$.
Montrer que, pour tous $i, j, k \in \llbracket 1, n \rrbracket$, on a $\alpha_{i,j} \alpha_{j,k} = \alpha_{i,k}$.

Si $\mathbf{d} = (d_1, \dots, d_n) \in (\mathbb{K}^*)^n$, on note $v_{\mathbf{d}}$ l'unique endomorphisme de E tel que $v_{\mathbf{d}}(e_k) = d_k e_k$, pour tout $k \in \llbracket 1, n \rrbracket$.

10. Montrer qu'un tel $v_{\mathbf{d}}$ est un automorphisme de E et que $\psi = \phi_{v_{\mathbf{d}}}$, pour un $\mathbf{d}$ à déterminer.
11. Déterminer l'ensemble $\mathcal{A}$.

3 Corps engendré par un nombre transcendant

Soit $\alpha \in \mathbb{C}$ un nombre transcendant, c'est-à-dire non algébrique.

On note $\mathbb{Q}(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)}, P \in \mathbb{Q}[X], Q \in \mathbb{Q}[X] \setminus \{0\} \right\}$.

1. Justifier que $\mathbb{Q}(\alpha)$ est bien défini et que tout élément $\beta \in \mathbb{Q}(\alpha)$ peut s'écrire $\beta = \frac{P(\alpha)}{Q(\alpha)}$, où $P \in \mathbb{Q}[X]$, $Q \in \mathbb{Q}[X] \setminus \{0\}$ et P et Q sont premiers entre eux.
2. Montrer que $\mathbb{Q}(\alpha)$ est un sous-corps et un sous- $\mathbb{Q}$ -espace vectoriel de $\mathbb{C}$.
3. Pour tout $q \in \mathbb{Q}$, on note $\beta_q = \frac{1}{\alpha - q}$. Montrer que la famille formée des β_q et des α^n , pour $q \in \mathbb{Q}$ et $n \in \mathbb{N}$, est une famille libre de $\mathbb{Q}(\alpha)$.

On cherche à déterminer les automorphismes de corps de $\mathbb{Q}(\alpha)$. Soit ϕ un tel automorphisme.

4. Montrer que ϕ est aussi un automorphisme linéaire de $\mathbb{Q}(\alpha)$.
5. On note $\beta = \phi(\alpha)$. Montrer que β est transcendant et que, pour tous $P \in \mathbb{Q}[X]$ et $Q \in \mathbb{Q}[X] \setminus \{0\}$,

$$\phi\left(\frac{P(\alpha)}{Q(\alpha)}\right) = \frac{P(\beta)}{Q(\beta)}.$$

6. En déduire qu'il existe $P \in \mathbb{Q}[X]$, $Q \in \mathbb{Q}[X] \setminus \{0\}$, avec $P \wedge Q = 1$, tels que $\frac{P(\beta)}{Q(\beta)} = \alpha$.

On écrit β sous la forme $\frac{A(\alpha)}{B(\alpha)}$, avec $A \in \mathbb{Q}[X]$, $B \in \mathbb{Q}[X] \setminus \{0\}$, $A \wedge B = 1$. On note d le

maximum des degrés de P et Q , $P = \sum_{j=0}^d p_j X^j$ et $Q = \sum_{k=0}^d q_k X^k$.

$$7. \text{ Montrer que } \sum_{j=0}^d p_j A^j B^{d-j} = X \sum_{k=0}^d q_k A^k B^{d-k}.$$

8. Montrer que A divise $(p_0 - q_0 X)B^d$. En déduire que A est de degré 0 ou 1.

9. Montrer que B est de degré 0 ou 1.

10. En déduire que β est de la forme $\frac{a\alpha + b}{c\alpha + d}$, avec $a, b, c, d \in \mathbb{Q}$ tels que $ad - bc \neq 0$.

11. Déterminer l'ensemble des automorphismes de corps de $\mathbb{Q}(\alpha)$.