DM 13 – Nombres algébriques

Les espaces vectoriels considérés dans ce problème sont définis sur le corps $\mathbb{Q}$ des nombres rationnels.

On dit qu'un espace vectoriel E est *de dimension finie* s'il admet une partie génératrice finie – c'est-à-dire s'il existe une partie finie $A \subset E$ telle que $E = \text{Vect}(A)$. On admet (provisoirement) qu'un sous-espace vectoriel d'un espace vectoriel de dimension finie est de dimension finie.

1 L'algèbre $\mathbb{Q}[\alpha]$

Soit α un nombre complexe. On note ϕ_α l'application définie de $\mathbb{Q}[X]$ dans $\mathbb{C}$ par $\phi_\alpha(P) = P(\alpha)$.

1. Montrer que ϕ_α est un morphisme d'anneaux et une application linéaire.
2. On note $\mathbb{Q}[\alpha]$ l'image de ϕ_α. Montrer que c'est un sous-anneau de $\mathbb{C}$ et que c'est le $\mathbb{Q}$-espace vectoriel engendré par $\{\alpha^n, n \in \mathbb{N}\}$.
3. Montrer l'équivalence entre les assertions suivantes :
   i) $\mathbb{Q}[\alpha]$ est de dimension finie.
   ii) Il existe $d \in \mathbb{N}$ tel que $\alpha^d \in \text{Vect}\left(\alpha^k, k \in [\![0, d-1]\!]\right)$.
   iii) ϕ_α n'est pas injectif.

   On dit que α est *algébrique* si ces conditions sont vérifiées, *transcendant* sinon.
4. Soit α un nombre algébrique. Montrer que $\text{Ker}\,\phi_\alpha$ est un idéal de $\mathbb{Q}[X]$. En déduire qu'il existe un unique polynôme unitaire $P_\alpha \in \mathbb{Q}[X]$ tel que $\text{Ker}\,\phi_\alpha = \{P_\alpha Q, Q \in \mathbb{Q}[X]\}$.

   On dit que P_α est le *polynôme minimal de* α. On dit que α est *de degré* d si P_α est de degré d.
5. Montrer que si α est algébrique, alors P_α est irréductible dans $\mathbb{Q}[X]$.
6. Déterminer les nombres algébriques de degré 1.
7. Montrer que $\alpha \in \mathbb{C}$ est algébrique de degré 2 ssi α est racine d'un trinôme $X^2 + mx + p \in \mathbb{Q}[X]$, dont le discriminant n'est pas le carré d'un rationnel.
8. On suppose que α est algébrique.
   (a) Soit $\beta \in \mathbb{Q}[\alpha] \setminus \{0\}$. Montrer que la multiplication par β, $m_\beta : \mathbb{C} \to \mathbb{C}, z \mapsto \beta z$ induit un automorphisme de $\mathbb{Q}[\alpha]$. *Pour la surjectivité, introduire une relation de Bézout.*
   (b) En déduire que $\mathbb{Q}[\alpha]$ est un corps.
9. Montrer réciproquement que si $\mathbb{Q}[\alpha]$ est un corps, alors α est algébrique.

Dans la suite, on note $\overline{\mathbb{Q}} \subset \mathbb{C}$ l'ensemble des nombres algébriques.

2 Le corps $\overline{\mathbb{Q}}$ des nombres algébriques

10. Soient α, β deux nombres algébriques, de degré respectif d et d'. On note $\mathbb{Q}[\alpha,\beta]$ le $\mathbb{Q}$-espace vectoriel engendré par $\{\alpha^k\beta^\ell, (k,\ell)\in\mathbb{N}^2\}$.
    (a) Montrer que $\mathbb{Q}[\alpha,\beta]$ est engendré par $\{\alpha^k\beta^\ell, (k,\ell)\in[\![0,d-1]\!]\times[\![0,d'-1]\!]\}$.
    (b) En déduire que $\alpha+\beta$ et $\alpha\beta$ sont algébriques.
11. Montrer que $\overline{\mathbb{Q}}$ est un corps.
12. Montrer que $\overline{\mathbb{Q}}$ est de plus *stable par radicaux*[1] : $\forall\alpha\in\mathbb{C}, \forall n\in\mathbb{N}^*, \alpha^n\in\overline{\mathbb{Q}} \implies \alpha\in\overline{\mathbb{Q}}$.

3 Mesure d'irrationalité et constante de Liouville (*facultatif*)

Soit x un nombre réel. La *mesure d'irrationalité* de x – notée $\mu(x)$ – est la borne inférieure de l'ensemble $\mathscr{A}_x$ des réels μ pour lesquels : $\exists A>0, \forall p\in\mathbb{Z}, \forall q\in\mathbb{N}^*, x\neq\dfrac{p}{q} \implies |x-\dfrac{p}{q}|\geq\dfrac{A}{q^\mu}$.
On convient que, si aucun μ ne vérifie cette condition, alors la mesure d'irrationalité de x est $+\infty$.

13. Montrer que $\mu(x)\geq 1$, avec égalité si $x\in\mathbb{Q}$.
14. On suppose que x est algébrique de degré $d\geq 2$ et on souhaite montrer que $\mu(x)\leq d$.[2]
    (a) Justifier qu'il existe un polynôme P à coefficients entiers, de degré d, sans racine rationnelle tel que $P(x)=0$.
    (b) Soit $(p,q)\in\mathbb{Z}\times\mathbb{N}^*$. On suppose que $\dfrac{p}{q}\in[x-1,x+1]$.
    Montrer qu'il existe $M>0$, indépendant de p et q, tel que $\left|P\left(\dfrac{p}{q}\right)\right|\leq M\left|x-\dfrac{p}{q}\right|$.
    (c) Montrer que $q^dP\left(\dfrac{p}{q}\right)\in\mathbb{Z}\setminus\{0\}$, puis que $\left|x-\dfrac{p}{q}\right|\geq\dfrac{1}{Mq^d}$.
    (d) En déduire que $\mu(x)\leq d$.

Ainsi, les nombres de Liouville sont transcendants.

15. Montrer qu'un réel x est un nombre de Liouville ssi pour tout $d\in\mathbb{R}$, il existe une infinité de couples $(p,q)\in\mathbb{Z}\times\mathbb{N}^*$ tels que $0<\left|x-\dfrac{p}{q}\right|<\dfrac{1}{q^d}$.
16. En déduire qu'un réel x est un nombre de Liouville ssi
$$\forall n\in\mathbb{N}, \exists(p_n,q_n)\in\mathbb{Z}\times[\![2,+\infty[\![, 0<\left|x-\frac{p_n}{q_n}\right|<\frac{1}{q_n^n}.$$
17. On note $\mathscr{L}=\lim\limits_{n\to+\infty}\sum\limits_{k=0}^{n}\dfrac{1}{10^{k!}}$ la constante de Liouville[3].
    Montrer que $\mathscr{L}$ est bien définie et que $\mu(\mathscr{L})=+\infty$.

[1] On peut s'intéresser au plus petit sous-corps $\mathbb{K}$ de $\mathbb{C}$ stable par radicaux. Il résulte des travaux d'Abel et Galois que $\mathbb{K}$ est *strictement* inclus dans $\overline{\mathbb{Q}}$. Ainsi certaines *racines* de polynômes ne s'expriment pas en extrayant des *racines*.

[2] En fait, la mesure d'irrationalité d'un réel algébrique irrationnel est toujours égale à 2. Ce théorème, démontré par Klaus Roth (1925-2015) en 1955, lui a valu la médaille Fields.

[3] D'après Joseph Liouville (1809-1882), qui a donné cet exemple parmi d'autres en 1844.