

DM 15 - 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 les deux faits suivants :

- Un sous-espace vectoriel d'un espace vectoriel de dimension finie est de dimension finie.
- Si f est un endomorphisme d'un espace vectoriel E de dimension finie, f est un automorphisme de E ssi f est injective ssi f est surjective.

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 $\alpha^d \in \text{Vect}(\alpha^k, k \in \llbracket 0, d-1 \rrbracket)$.
 - 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 $\mathbb{Q}[X]$.

On en déduit qu'il existe un unique polynôme unitaire $P_\alpha \in \mathbb{Q}[X]$ tel que $\text{Ker } \phi_\alpha$ est l'idéal $P_\alpha \mathbb{Q}[X] = \{P_\alpha Q, Q \in \mathbb{Q}[X]\}$. C'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 , $m_\beta : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto \beta z$ induit un endomorphisme injectif de $\mathbb{Q}[\alpha]$.
- (b) Justifier que cet endomorphisme est un automorphisme. En déduire que $\mathbb{Q}[\alpha]$ est un corps.

9. Montrer réciproquement que si $\mathbb{Q}[\alpha]$ est un corps, alors α est algébrique.

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

On note $\overline{\mathbb{Q}} \subset \mathbb{C}$ l'ensemble 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 $\{\alpha^k \beta^\ell, (k, \ell) \in \llbracket 0, d-1 \rrbracket \times \llbracket 0, d'-1 \rrbracket\}$.
- (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 $\overline{\mathbb{Q}}$ est dénombrable

On rappelle qu'un ensemble E est *dénombrable* s'il existe une surjection $\phi : \mathbb{N} \rightarrow E$.

On admet que \mathbb{Z} , \mathbb{N}^2 et les ensembles finis sont dénombrables.

13. Montrer que \mathbb{Q} est dénombrable.

14. Soient $n \in \mathbb{N}^*$, soient E_1, \dots, E_n des ensembles dénombrables.
Montrer que $E_1 \times \dots \times E_n$ est dénombrable.

15. Soient A un ensemble dénombrable et $(E_a)_{a \in A}$ une famille d'ensemble dénombrables.
Montrer que $E = \bigcup_{a \in A} E_a$ est dénombrable.

16. En déduire que $\overline{\mathbb{Q}}$ est dénombrable.

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

Dans cette partie, on définit la constante de Liouville², premier exemple historique de nombre transcendant.

¹On 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*.

²d'après Joseph Liouville (1809-1882), qui a donné cet exemple parmi d'autres en 1844. L'existence de nombres transcendants se déduit de la partie précédente – car \mathbb{R} n'est pas dénombrable – mais il est en général difficile de montrer qu'un nombre donné est transcendant.

Soit x un nombre réel. La *mesure d'irrationalité* de x – notée $\mu(x)$ – est la borne inférieure de l'ensemble \mathcal{A}_x des réels μ pour lesquels

$$\exists A > 0, \forall p \in \mathbb{Z}, \forall q \in \mathbb{N}^*, x \neq \frac{p}{q} \implies \left| x - \frac{p}{q} \right| \geq \frac{A}{q^\mu}.$$

On convient que, si aucun μ ne vérifie cette condition, alors la mesure d'irrationalité de x est $+\infty$: un tel nombre est un *nombre de Liouville*.

17. Montrer que $\mu(x) \geq 1$, avec égalité si $x \in \mathbb{Q}$.
18. On suppose que x est algébrique de degré $d \geq 2$ et on souhaite montrer que $\mu(x) \leq d$.³
 - (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 $\frac{p}{q} \in [x - 1, x + 1]$. Montrer qu'il existe $M > 0$, indépendant de p et q , tel que $\left| P\left(\frac{p}{q}\right) \right| \leq M \left| x - \frac{p}{q} \right|$.
 - (c) Montrer que $q^d P\left(\frac{p}{q}\right) \in \mathbb{Z} - \{0\}$, puis que $\left| x - \frac{p}{q} \right| \geq \frac{1}{Mq^d}$.
 - (d) En déduire que $\mu(x) \leq d$.

Ainsi, les nombres de Liouville sont transcendants.

19. 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 $0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^d}$.
20. En déduire qu'un réel x est un nombre de Liouville ssi

$$\forall n \in \mathbb{N}, \exists (p_n, q_n) \in \mathbb{Z} \times \llbracket 2, +\infty[, 0 < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n}.$$

On note $\mathcal{L} = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{1}{10^{k!}}$ la constante de Liouville.

21. Montrer que \mathcal{L} est bien définie et que c'est un nombre de Liouville.

³En 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.