POLYNÔME MINIMAL ET ÉLÉMENTS ALGÉBRIQUES

Définitions et notations:

- $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.
- On appelle $\mathbb{K}$-algèbre tout quadruplet $(\mathbb{A},+,\times,.)$ tel que $(\mathbb{A},+,\times)$ un anneau, $(\mathbb{A},+,.)$ un $\mathbb{K}$-espace vectoriel et

$$\forall x,y\in\mathbb{A} \text{ et } \lambda\in\mathbb{K},\quad \lambda.(a\times b)=(\lambda.a)\times=a\times(\lambda.b)$$

  Si de plus la loi $\times$ est commutative on parle d'algèbre commutative.
- $(\mathbb{C},+,\times,.)$ est une $\mathbb{K}$-algèbre commutative
- $(\mathbb{K}[X],+,\times,.)$ est une $\mathbb{K}$-algèbre intègre.
- Soit $(\mathbb{A},+,\times,.)$ une $\mathbb{K}$-algèbre et $\mathbb{B}\subset\mathbb{A}$. On dit $\mathbb{B}$ est une sous-algèbre de $(\mathbb{A},+,\times,.)$ si:
  - $1_A\in\mathbb{B}$
  - $\forall x,y\in\mathbb{B},\forall\alpha,\beta\in\mathbb{K}\quad \alpha x+\beta y\in\mathbb{B}$
  - $\forall x,y\in\mathbb{B},\quad x\times y\in\mathbb{B}$

  Alors munie des lois restreintes, $\mathbb{B}$ est une $\mathbb{K}$-algèbre.
- Soit $(\mathbb{A},+,\times,.)$ et $(\mathbb{A}',+,\times,.)$ deux $\mathbb{K}$-algèbres. On appelle morphisme d'algèbres, de $\mathbb{A}$ à valeurs dans $\mathbb{A}'$, toute application $f:\mathbb{A}\longrightarrow\mathbb{A}'$ telle que
  - $f(1_{\mathbb{A}})=1_{\mathbb{A}'}$
  - Pour tous $x,y\in\mathbb{A}$ et $\lambda\in\mathbb{K}$:

$$f(\lambda x+y)=\lambda f(x)+f(y)\quad\text{et}\quad f(x\times y)=f(x)\times f(y)$$

- Un isomorphisme d'algèbres est un morphisme d'algèbres bijectif.
- Un automorphisme d'algèbres est un endomorphisme d'algèbres bijectif.
- Deux $\mathbb{K}$-algèbres sont dites isomorphes si, et seulement si, il existe un isomorphisme d'algèbres de l'une vers l'autre.
- Pour $P=\sum_{k=0}^{n}a_kX^k\in\mathbb{K}[X]$ et $a\in\mathbb{A}$, on définit la valeur de P en a, par $P(a)=\sum_{k=0}^{n}a_ka^k\in\mathbb{A}$

Dans ce problème $\mathbb{A}$ désigne une $\mathbb{K}$-algèbre non nulle et $a\in A$. On définit :

$$\varphi_a:\begin{cases}\mathbb{K}[X] & \longrightarrow & \mathbb{A}\\ P & \longmapsto & P(a)\end{cases}$$

Partie I: Algèbre monogène

1. Montrer que φ_a est un morphisme d'algèbres, appelé morphisme d'évaluation en a.
2. Montrer que $\mathrm{Im}\,(\varphi_a)=\{P(a)\mid P\in\mathbb{K}[X]\}$ est une sous-algèbre commutative de $\mathbb{A}$ contenant a notée $\mathbb{K}[a]$
3. Montrer que $\mathbb{K}[a]$ est la plus petite sous-algèbre de $\mathbb{A}$ (au sens de l'inclusion) contenant a; appelée la sous-algèbre engendrée par a.
4. Montrer que $I_a=\mathrm{Ker}\,(\varphi_a)=\{P\in\mathbb{K}[X]\ ,\ P(a)=0\}$ est un idéal de $\mathbb{K}[X]$, appelé l'idéal annulateur de a et tout polynôme de I_a est dit polynôme annulateur de a.
5. Si φ_a est injectif, montrer que $\mathbb{K}[a]$ est isomorphe à $\mathbb{K}[X]$.

Partie II: Polynôme minimal

Dans cette partie, on suppose que φ_a n'est pas injectif.

6. Expliquer qu'il existe un unique polynôme unitaire $\pi_a \in \mathbb{K}[X]$ tel que $\operatorname{Ker}(\varphi_a) = \pi_a.\mathbb{K}[X]$.
   Ce polynôme est appelé le polynôme minimal de a.
7. Montrer que $\deg(\pi_a) \geqslant 1$.
8. Posons $d = \deg(\pi_a)$.
   (a) Montrer que la famille $(a^k)_{0\leqslant k\leqslant d-1}$ est libre dans $\mathbb{K}[a]$
   (b) En utilisant la division euclidienne, montrer que $(a^k)_{0\leqslant k\leqslant d-1}$ est génératrice de $\mathbb{K}[a]$
   (c) En déduire $\dim_{\mathbb{K}} \mathbb{K}[a]$.
9. Soit $\beta \in \mathbb{K}[a]$ et $Q \in \mathbb{K}[X]$ tels que $\beta = Q(a)$.
   Montrer que β est inversible dans $\mathbb{K}[a]$ si, et seulement si, $Q \wedge \pi_a = 1$.
10. Montrer que les trois assertions suivantes sont équivalentes
    (a) $\mathbb{K}[a]$ est intègre.
    (b) $\mathbb{K}[a]$ est un corps.
    (c) π_a est irréductible sur $\mathbb{K}$.
11. Soit $\mathbb{L}$ un sur-corps de $\mathbb{K}$ et soit E un $\mathbb{L}$-espace vectoriel.
    (a) Expliquer que $\mathbb{L}$ et E sont des $\mathbb{K}$-espaces vectoriels.
    (b) Dans le cas des dimensions finies. Montrer que $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} \mathbb{L}.\dim_{\mathbb{L}} E$.

Partie III: Éléments algébriques

On dit qu'un élément $a \in \mathbb{C}$ est algébrique sur $\mathbb{K}$ si $I_a \neq \{0\}$, on dit qu'il est transcendant sur $\mathbb{K}$ sinon. Dans le premier cas, on dit que a est algébrique de degré le degré de π_a.

12. Montrer que tout élément de $\mathbb{C}$ est algébrique sur $\mathbb{R}$ de degré inférieur ou égal à 2.
13. Expliquer que a est algébrique sur $\mathbb{K}$ si, et seulement si, $\mathbb{K}[a]$ est un espace vectoriel de dimension finie sur $\mathbb{K}$.
14. Soit $a = j + \sqrt{3} \in \mathbb{C}$
    (a) Montrer que a est algébrique sur $\mathbb{Q}$ et calculer son polynôme minimal.
    (b) Expliquer que $\mathbb{Q}[j]$ et $\mathbb{Q}[\sqrt{3}]$ sont des corps, puis montrer que $(\mathbb{Q}[\sqrt{3}])[j] = (Q[j])[\sqrt{3}] = Q[a]$.
15. Notons $\mathbb{L} = \{x \in \mathbb{C},\ x \text{ algébrique sur } \mathbb{Q}\}$. On souhaite montrer que c'est un sous-corps de $\mathbb{C}$.
    (a) Montrer que si $a \in \mathbb{L}$ alors $-a \in \mathbb{L}$.
    (b) Montrer que si $a, b \in \mathbb{L}$, alors $(Q[a])[b]$ est de dimension finie sur $\mathbb{Q}$. En déduire que $a+b$ et $a.b$ appartiennent à $\mathbb{L}$.
    (c) Montrer que si $P \in \mathbb{Q}[X]$ est de degré d alors $X^d P\left(\dfrac{1}{X}\right) \in \mathbb{Q}[X]$. En déduire que si $a \in L \setminus \{0\}$ alors $\dfrac{1}{a} \in \mathbb{L}$.
    (d) Conclure.
16. Soit $(z_0, \cdots, z_n) \in \mathbb{L}^{n+1}$ et $\zeta \in \mathbb{C}$ racine de $P = \displaystyle\sum_{k=0}^{n} z_k X^k$. Montrer que $\zeta \in L$. Conclure.