MP2I du lycée Victor Hugo de Besançon,
Année scolaire 2024/2025.

Problème : extensions de corps et nombres algébriques

Soit L un corps, et K un sous-corps de L, *i.e.* $K \subset L$ et K est un corps pour les mêmes lois que L. On peut alors munir L d'une structure de K-espace vectoriel, où l'addition est l'addition de L, et la multiplication par les scalaires est définie pour $\lambda \in K$ et $x \in L$ par $\lambda \cdot x$, où $\cdot$ est la multiplication dans L.

Dans le cas où L est de dimension finie sur K, on dit que L est une extension finie de K, et on note $[L : K] = \dim_K(L)$.

Partie 1 : premiers exemples

1. (a) Montrez que $\mathbb{C}$ est une extension finie de $\mathbb{R}$, et déterminez $[\mathbb{C} : \mathbb{R}]$.
   (b) Déterminez tous les sous-corps de $\mathbb{C}$ qui contiennent $\mathbb{R}$.
2. On rappelle que $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ est un sous-corps de $\mathbb{R}$, et donc un corps. Montrez que $\mathbb{Q}(\sqrt{2})$ est une extension finie de $\mathbb{Q}$ et déterminez $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.
3. Soit $\mathbb{Q}(\sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\right\}$. On admet que c'est un sous-corps de $\mathbb{R}$ et que $\sqrt[3]{2}$ est irrationnel.
   (a) On veut montrer que $\sqrt[3]{2}$ n'est pas racine d'un polynôme $P \in \mathbb{Q}_2[X]$, $P \neq 0$. On raisonne par l'absurde, et on suppose qu'il existe $P \in \mathbb{Q}_2[X]$, $P \neq 0$, tel que $P(\sqrt[3]{2}) = 0$.
      i. Montrez que P divise $X^3 - 2$.
      ii. En utilisant la forme scindée de $X^3 - 2$ dans $\mathbb{C}[X]$, aboutir à une contradiction.
   (b) En déduire que $\mathbb{Q}(\sqrt[3]{2})$ est une extension finie de $\mathbb{Q}$ et déterminez $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.
4. Soient $k \subset K \subset L$ trois corps. On suppose que K est une extension finie de k et L une extension finie de K.

   Soit $(\alpha_1, \ldots, \alpha_n)$ une base du k-espace vectoriel K, et $(\beta_1, \ldots, \beta_p)$ une base du K-espace vectoriel L. Montrez que $(\alpha_i\beta_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ est une base du k-espace vectoriel L.

   En déduire que L est une extension finie de k et que $[L : k] = [L : K][K : k]$.

Partie 2 : éléments algébriques

Dans cette partie, on fixe $K \subset L$ deux corps. Pour $a \in L$, on note $K[a] = \text{vect}_K(a^n)_{n\in\mathbb{N}}$ le sous K-espace vectoriel du K-espace vectoriel L engendré par la famille $(a^n)_{n\in\mathbb{N}}$.

L'élément a est algébrique sur K s'il existe $P \in K[X]$, non nul, tel que $P(a) = 0$.

1. Soit $a \in L$. Montrez que $K[a] = \{P(a) \mid P \in K[X]\}$. En déduire que $K[a]$ est un sous-anneau de L. Montrez que c'est le plus petit anneau de L contenant K et a, *i.e.* que si A est un sous-anneau de L tel que $a \in A$ et $K \subset A$, alors $K[a] \subset A$.
2. Soit $a \in L$. Montrez que a est algébrique sur K si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $(1, a, \cdots, a^n)$ soit liée dans le K-espace vectoriel L.

Si $a \in L$ est algébrique sur K, on appelle degré de a sur K le plus petit entier d tel que $(1, a, \cdots, a^d)$ soit liée dans le K-espace vectoriel L.

3. Montrez que $a \in L$ est algébrique sur K de degré 1 si et seulement si $a \in K$.
4. Montrez que si L est une extension finie de K, alors tout élément $a \in L$ est algébrique sur K de degré inférieur ou égal à $[L : K]$.
5. Soit $a \in L$ algébrique sur K de degré d.
   (a) Montrez que $(1, a, \cdots, a^{d-1})$ est une K-base de $K[a]$, *i.e.* une base du K-espace vectoriel $K[a]$.
   (b) Soit $b \in K[a]$, et soit $\begin{array}{rccc} f_b : & K[a] & \longrightarrow & K[a] \\ & x & \longmapsto & bx \end{array}$. Montrez que si $b \neq 0$, alors f_b est un automorphisme du K-espace vectoriel $K[a]$.
   (c) En déduire que $K[a]$ est un sous-corps de L, et que c'est le plus petit sous-corps de L contenant a et K.
   (d) Montrez que $K[a]$ est une extension finie de K et déterminez $[K[a] : K]$.
   (e) Montrez que $\mathbb{Q}(\sqrt[3]{2})$ est un sous-corps de $\mathbb{R}$.

   La notation $K(a)$ désigne le plus petit sous-corps de L contenant K et a. Lorsque a est algébrique, on a donc $K[a] = K(a)$, d'où les notations $\mathbb{Q}(\sqrt{2})$ etc...

   (f) Soit $a \in L$, $a \neq 0$. Montrez qu'il y a équivalence entre :
      i. $K[a]$ est un sous-corps de L.
      ii. $a^{-1} \in K[a]$.
      iii. a est algébrique sur K.

Partie 3 : polynôme minimal d'un élément algébrique

Dans cette partie, on considère deux corps $K \subset L$. On considère un élément $a \in L$, algébrique sur K de degré d.

On note $I_a = \{P \in K[X] \mid P(a) = 0\}$. Comme a est algébrique, I_a n'est pas réduit au polynôme nul. On note q le plus petit degré d'un polynôme $P \neq 0$ de I_a : $q = \min(\{\deg(P) \mid P \in I_a,\ P \neq 0\})$.

1. Montrez que I_a contient un unique polynôme unitaire de degré q.

   On l'appelle polynôme minimal de a, et on le note μ_a.

2. Montrez que μ_a est irréductible dans $K[X]$, et que $I_a = \{\mu_a Q \mid Q \in K[X]\}$.
3. Montrez que $q = d$.
4. Quel est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$?
5. Montrez que $\sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbb{Q}$ et déterminez le degré de son polynôme minimal.

Partie 4 : nombres algébriques

Dans cette partie, un nombre algébrique est un nombre complexe algébrique sur $\mathbb{Q}$. On note $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques :

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} \mid \exists\, P \in \mathbb{Q}[X] \mid P \neq 0,\ P(a) = 0\}.$$

1. Soient $a, b \in \overline{\mathbb{Q}}$. On rappelle que $\mathbb{Q}[a]$ est un corps, et on note $\mathbb{Q}[a, b] = (\mathbb{Q}[a])[b]$.
   (a) Montrez que $\mathbb{Q}[a, b]$ est un corps, et que c'est une extension finie de $\mathbb{Q}$.
   (b) Exemple : montrez que $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\right\}$.
2. Montrez que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.