Problème : extensions de corps et nombres algébriques

Partie 1 : premiers exemples

1. (a) $(1, i)$ est une $\mathbb{R}$-base de $\mathbb{C}$, donc $\mathbb{C}$ est une extension finie de $\mathbb{R}$ et $\boxed{[\mathbb{C} : \mathbb{R}] = 2}$.
   (b) Soit L un corps tel que $\mathbb{R} \subset L \subset \mathbb{C}$. C'est donc un sous-espace vectoriel du $\mathbb{R}$-espace vectoriel $\mathbb{C}$, donc sa dimension est 1 ou 2. Si c'est 1, $L = \mathbb{R}$, sinon, $L = \mathbb{C}$.
2. On montre que $(1, \sqrt{2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$. Par définition, c'est une famille génératrice. Or, elle est libre (fait en td), donc c'est une base, donc $\mathbb{Q}(\sqrt{2})$ est une extension finie de qq et $\boxed{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2}$.
3. (a) i. On effectue la division euclidienne de $X^3 - 2$ par P. Comme ce sont des polynômes de $\mathbb{Q}[X]$, il existe $A, R \in \mathbb{Q}[X]$ tels que $X^3 - 2 = AP + R$, avec $\deg(R) \leqslant 1$. Mais alors $R(\sqrt[3]{2}) = 0$, donc $R = 0$ car $\sqrt[3]{2} \notin \mathbb{Q}$ et $R \in \mathbb{Q}_1[X]$.
   ii. Mais $X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$ qui est un produit d'irréductibles, donc P est un produit d'au plus deux de ces polynômes irréductibles, et $P \notin \mathbb{Q}[X]$: contradiction.
   (b) Montrons que $(1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{2})$. Par définition, elle est génératrice. Soient alors $a, b, c \in \mathbb{Q}$ tels que $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 = 0$. Alors $P = a + bX + cX^2 \in \mathbb{Q}[X]$ admet $\sqrt[3]{2}$ pour racine, donc $P = 0$, et $a = b = c = 0$: la famille est libre, c'est bien une $\mathbb{Q}$-base, et $\mathbb{Q}(\sqrt[3]{2})$ est une extension finie de $\mathbb{Q}$, et $\boxed{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3}$.
4. Soit $v \in L$. Il existe $(v_1, \cdots, v_p) \in K^p$ tel que $v = \sum_{j=1}^{p} v_j \beta_j$. Or, $(\alpha_1, \ldots, \alpha_n)$ est une k base de K, donc pour tout $j = 1, \cdots, p$, il existe $\lambda_{ij} \in k$ tel que $v_j = \sum_{i=1}^{n} \lambda_{ij}\alpha_i$, et donc

$$v = \sum_{j=1}^{p} \left(\sum_{i=1}^{n} \lambda_{ij}\alpha_i \right) \beta_j = \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{ij}\alpha_i\beta_j,$$

donc la famille $(\alpha_i\beta_j)_{i,j}$ est génératrice du k-espace vectoriel L.

Considérons alors une famille $(\lambda_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ d'éléments de k tels que $\sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{ij}\alpha_i\beta_j = 0$. On a alors

$$\sum_{j=1}^{p} \left(\sum_{i=1}^{n} \lambda_{ij}\alpha_i \right) \beta_j = 0.$$

Or, $\lambda_{ij} \in k$, $\alpha_i \in K$, donc $\sum_{i=1}^{n} \lambda_{ij}\alpha_i \in K$, et $(\beta_1, \ldots, \beta_p)$ est K-libre, donc :

$$\forall\, j = 1, \ldots, p,\ \sum_{i=1}^{n} \lambda_{ij}\alpha_i = 0.$$

Mais $(\alpha_1, \ldots, \alpha_n)$ est k-libre, donc pour tous i, j, $\lambda_{ij} = 0$, et la famille $(\alpha_i\beta_j)$ est k-libre : c'est une k-base de L, qui est donc une extension finie de k, de dimension np.

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. Par définition de $K[a]$, c'est l'ensemble des combinaisons linéaires finies à coefficients dans K des puissances de a, donc l'ensemble $P(a)$ où $P \in K[X]$.

   Or, si $P, Q \in K[X]$, alors $P(a)Q(a) = (PQ)(a) \in K[a]$, qui est donc bien un sous-anneau de L.

   Enfin, si A est un sous-anneau de L contenant K et a, par stabilité par produit, il contient toutes les puissances de a, et tous les produits d'éléments de K par une puissance de a, et par stabilité par somme, toutes les combinaisons linéaires à coefficients dans K des puissances de a, *i.e.* $K[a]$.
2. Par définition, on a

$$\begin{aligned} a \text{ algébrique sur } K &\iff \exists\, P \in K[X],\ P \neq 0 \mid P(a) = 0 \\ &\iff \exists\, n \in \mathbb{N}^*,\ (\lambda_0, \dots \lambda_n) \in K^{n+1},\ \text{non tous nuls} \mid \sum_{i=0}^{n} \lambda_i a^i = 0 \\ &\iff \exists\, n \in \mathbb{N}^* \mid (1, a, \cdots, a^n) \text{ liée} \end{aligned}$$

3. Soit $a \in L$. Alors :

$$\begin{aligned} a \text{ est algébrique sur } K \text{ de degré } 1 &\iff \exists\, (\lambda, \mu) \in K^2,\ (\lambda, \mu) \neq (0,0) \mid \lambda + \mu a = 0 \\ &\overset{a\neq 0}{\iff} \exists\, (\lambda, \mu) \in K^2,\ \mu \neq 0 \mid \lambda + \mu a = 0 \\ &\iff \exists\, (\lambda, \mu) \in K^2,\ \mu \neq 0 \mid a = \mu^{-1}\lambda \\ &\iff a \in K. \end{aligned}$$

4. Soit $a \in L$. Alors $K[a]$ est un sous K-espace vectoriel de L, et est donc de dimension finie. La famille $(a^n)_{n\in\mathbb{N}}$ est donc liée, et a est algébrique.

   Soit alors d le degré de a. Alors $(1, a, \cdots, a^{d-1})$ est une famille K-libre, donc $d \leqslant [L : K]$.
5. Soit $a \in L$ algébrique sur K de degré d.
   (a) Par définition de d, c'est une famille libre, et $a^d \in \text{vect}(1, a, \cdots, a^{d-1})$: il existe $P \in K_{d-1}[X]$ tel que $a^d = P(a)$. Pour un $n \geqslant d$, on a alors

$$a^n = a^{n-d}P(a) \in \text{vect}(a^k)_{0\leqslant k\leqslant n-1}.$$

   Par récurrence, on a ainsi pour $n \geqslant d$, $\text{vect}(a^k)_{0\leqslant k\leqslant n} \in \text{vect}(a^k)_{0\leqslant k\leqslant d-1}$, ce qui prouve que la famille $(a^k)_{0\leqslant k\leqslant d-1}$ est une famille génératrice, donc une base de $K[a]$.

   (b) Déjà, f_b est bien définie car $K[a]$ est un sous-anneau de L. Puis, comme $K[a]$ est un K-espace vectoriel de dimension finie, il suffit de montrer que f_b est linéaire et injective. Mais la linéarité découle de la ditributivité et de la commutativité dans L. Enfin, si $x \in \text{Ker}(f_b)$, alors $bx = 0$, et comme $b \neq 0$, on a $x = 0$ (L est un corps), donc $\text{Ker}(f_b) = \{0\}$ et f_b est injective.

   (c) Pour montrer que $K[a]$ est un sous-corps de L, il reste à montrer que si $b \in K[x]$ et $b \neq 0$, alors $b^{-1} \in K[a]$. Or, $1 \in K[a]$, et f_b est un automorphisme de $K[a]$, donc $b^{-1} = f_b^{-1}(1) \in K[a]$.

   (d) D'après 5(a) et 5(c), $K[a]$ est une extension finie de K, et $\boxed{[K[a] : K] = \deg(a)}$.

   (e) $\mathbb{Q}(\sqrt[3]{2})$ défini dans la partie 1 est en fait $\mathbb{Q}[\sqrt[3]{2}]$ comme défini ici. Or, $X^3 - 2$ est un polynôme à coefficients rationnels qui annule $\sqrt[3]{2}$, et donc $\mathbb{Q}[\sqrt[3]{2}]$ est un sous-corps de $\mathbb{R}$.

(f) — i ⇒ ii : si $K[a]$ est un sous-corps de L, comme $a \neq 0$, $a^{-1} \in K[a]$.
— ii ⇒ iii : Supposons que $a^{-1} \in K[a]$. Il existe donc $P \in K[X]$ tel que $a^{-1} = P(a)$, et donc $aP(a) - 1 = 0$, et $XP - 1 \in K[X]$ annule a, qui est donc algébrique.
— iii ⇒ i : si a est algébrique sur K, par 5, $K[a]$ est un sous-corps de L.

Partie 3 : polynôme minimal d'un élément algébrique

1. Par définition de q, il existe $P \in I_a$ de degré q, et $\mathrm{dom}(P)^{-1}P$ est unitaire, de degré q, et annule a.

   Montrons l'unicité. Soient $P, Q \in I_a$, unitaires de degré q. Alors $(P-Q)(a) = P(a) - Q(a) = 0$ donc $P - Q \in I_a$. Or, $\deg(P-Q) < q$ (P, Q de même degré et de même coefficients dominants), donc par définitino de q, $P - Q = 0$.
2. Supposons que $\mu_a = PQ$, avec $P, Q \in K[X]$. Alors $P(a)Q(a) = 0$, donc $P(a) = 0$ ou $Q(a) = 0$. Si par exemple $P(a) = 0$, alors $P \in I_a$. Mais $\deg(P) \leqslant q$, et $P \neq 0$ (car $\mu_a \neq 0$), donc par 1, $P \sim \mu_a$, et μ_a est irréductible dans $K[X]$.

   Enfin, si $Q \in K[X]$, on a $(\mu_a Q)(a) = \mu_a(a)Q(a) = 0$ donc $\mu_a Q \in I_a$.

   Réciproquement, si $P \in I_a$, en divisant P par μ_a, on a $P = \mu_a Q + R$, où $P, Q \in K[X]$, et $\deg(R) < q$. Mais $R(a) = 0$, donc $R \in I_a$, et $R = 0$.
3. C'est en fait la définition du degré : le plus petit entier tel que $(1, a, \cdots, a^d)$ est K-liée signifie le plus petit entier d tel qu'il existe un polynôme de degré d qui annule a : c'est le degré du polynôme minimal.
4. Montrons que c'est $\boxed{X^3 - 2}$. En effet, ce polynôme est unitaire et annule $\sqrt[3]{2}$. DE plus, on a montré en partie 1, Q3(b), que $[\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}] = 3$, qui est aussi le degré du polynôme minimal. Par unicité, $X^3 - 2$ est bien le polynôme cherché.
5. Soit $P = (X - \sqrt{2})^2 - 3 \in \mathbb{Q}[\sqrt{2}][X]$. Alors $P(\sqrt{2} + \sqrt{3}) = 0$, donc $\sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbb{Q}[\sqrt{2}]$, et $\big[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}[\sqrt{2}]\big] = 2$. Mais $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, donc par la partie 1, Q2, $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ est une extension finie de $\mathbb{Q}$ et $\big[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}\big] = \big[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}[\sqrt{2}]\big] \times \big[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\big] = 4$, donc $\boxed{\text{le degré du polynôme minimal est 4}}$.

Partie 4 : nombres algébriques

1. (a) Comme b est algébrique sur $\mathbb{Q}$, il l'est aussi sur $\mathbb{Q}[a]$, donc $\mathbb{Q}[a][b]$ est un corps, et est une extension finie de $\mathbb{Q}[a]$, et donc, comme $\mathbb{Q}[a]$ est une extension finie de $\mathbb{Q}$, par la partie 1, Q2, $\mathbb{Q}[a][b]$ est aussi une extension finie de $\mathbb{Q}$, et on a $[\mathbb{Q}[a, b], \mathbb{Q}] = [\mathbb{Q}[a, b] : \mathbb{Q}[a]] \times [\mathbb{Q}[a], \mathbb{Q}]$.

   (b) Notons $L = \big\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\big\}$. Comme $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ qui est un corps, on a $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, et donc par sommes et produits d'éléments du corps $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $L \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

   Réciproquement, tout élément de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ est une combinaison linéaire à coefficients rationnels de $\sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$, et de leurs puissances, donc $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
2. Montrons que $\overline{\mathbb{Q}}$ est stable par somme, produit, et passage à l'inverse. Soient $a, b \in \overline{\mathbb{Q}}$. Or, par 1(a), $\mathbb{Q}[a, b]$ est un corps, donc $a^{-1}, a+b, ab \in \mathbb{Q}[a, b]$. On en déduit par la partie 2, Q1, que $\mathbb{Q}[a^{-1}] \subset \mathbb{Q}[a, b]$, $\mathbb{Q}[a + b] \subset \mathbb{Q}[a, b]$, $\mathbb{Q}[ab] \subset \mathbb{Q}[a, b]$.

   Or, $\mathbb{Q}[a, b]$ est une extension finie de $\mathbb{Q}$ par 1(a), donc $\mathbb{Q}[a^{-1}]$, $\mathbb{Q}[a+b]$ et $\mathbb{Q}[ab]$ également, et donc par la partie 2, $a^{-1}, a + b, ab$ $\overline{\mathbb{Q}}$.