

Corrigé du contrôle de maths L3 : extensions de corps et corps finis

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours : la base télescopique	3 points
Exercice 2 : Degré de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ et polynôme minimal de $\sqrt{2} + \sqrt{3}$	5 points
Exercice 3 : Corps de décomposition de $X^3 - 2$	3 points
Exercice 4 : Corps finis F_4 et F_8 , cyclicité du groupe multiplicatif	5 points
Exercice 5 : Problème : la duplication du cube et la trisection	4 points
Total	20 points

Exercice 1 : Question de cours : la base télescopique (3 points)

- a. **Théorème de la base télescopique.** La famille $(e_i f_j)_{i,j}$ est une base de M sur K . En particulier, $[M : K] = [M : L][L : K]$.

Famille génératrice. Soit $x \in M$. On écrit d'abord $x = \sum_j \lambda_j f_j$ avec $\lambda_j \in L$. Ensuite, chaque λ_j s'écrit $\lambda_j = \sum_i \mu_{ij} e_i$ avec $\mu_{ij} \in K$. Donc $x = \sum_{i,j} \mu_{ij} e_i f_j$.

Famille libre. Supposons $\sum_{i,j} \mu_{ij} e_i f_j = 0$ avec $\mu_{ij} \in K$. On regroupe :

$\sum_j \left(\sum_i \mu_{ij} e_i \right) f_j = 0$, où les coefficients entre parenthèses sont dans L . Comme (f_j) est libre sur L , chaque $\sum_i \mu_{ij} e_i$ est nul. Puis, comme (e_i) est libre sur K , tous les μ_{ij} sont nuls.

Ainsi $[M : K] = nm$.

- b. D'après a), M est de dimension finie $N = nm$ sur K . La famille $1, \alpha, \dots, \alpha^N$ compte $N + 1$ vecteurs, donc elle est liée. Il existe ainsi un polynôme non nul de $K[X]$ qui annule α : α est algébrique sur K .

Son degré est $[K(\alpha) : K]$. On applique a) à $K \subset K(\alpha) \subset M$:
 $[M : K] = [M : K(\alpha)] [K(\alpha) : K]$. Donc le degré de α divise $[M : K]$.

Barème : a) 0,5 point pour l'énoncé, 0,75 point pour le caractère générateur, 0,75 point pour la liberté ; b) 0,5 point pour le caractère algébrique, 0,5 point pour la divisibilité.

Exercice 2 : Degré de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ et polynôme minimal de $\sqrt{2} + \sqrt{3}$ (5 points)

- a. Supposons $\sqrt{3} = a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. En élevant au carré, on obtient
 $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Comme $\sqrt{2}$ est irrationnel, on a $ab = 0$.

Si $b = 0$, alors $\sqrt{3} = a$ serait rationnel : c'est faux. Si $a = 0$, alors $b^2 = \frac{3}{2}$, donc $\sqrt{6} = |2b|$ serait rationnel : c'est faux aussi. **Donc** $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

- b. Le polynôme $X^2 - 2$ est de degré 2 sans racine rationnelle, donc irréductible. Ainsi
 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, avec la base $(1, \sqrt{2})$.

De même, $X^2 - 3$ n'a pas de racine dans $\mathbb{Q}(\sqrt{2})$ d'après a). Il y est donc irréductible, et
 $[L : \mathbb{Q}(\sqrt{2})] = 2$, avec la base $(1, \sqrt{3})$.

Par le théorème de la base télescopique, $[L : \mathbb{Q}] = 4$, avec la base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$.

c. On calcule $\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$. Donc $(\alpha^2 - 5)^2 = 24$, soit $\alpha^4 - 10\alpha^2 + 25 = 24$. **Le polynôme $P = X^4 - 10X^2 + 1$ convient.**

d. On développe :

$$\alpha^3 = 2\sqrt{2} + 3 \times 2 \times \sqrt{3} + 3 \times \sqrt{2} \times 3 + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}.$$

Ainsi $\alpha^3 - 9\alpha = 2\sqrt{2}$ et $11\alpha - \alpha^3 = 2\sqrt{3}$. Donc $\sqrt{2} = \frac{\alpha^3 - 9\alpha}{2}$ et $\sqrt{3} = \frac{11\alpha - \alpha^3}{2}$ appartiennent à $\mathbb{Q}(\alpha)$.

On en déduit $L \subset \mathbb{Q}(\alpha)$. L'inclusion inverse est claire, donc $\mathbb{Q}(\alpha) = L$. Le degré de α vaut alors 4. Le polynôme minimal divise P , il est unitaire et de même degré. **Le polynôme minimal de α est $X^4 - 10X^2 + 1$.**

Barème : a) 1 point ; b) 0,5 point pour chaque degré intermédiaire, 0,5 point pour la base ; c) 1 point ; d) 0,5 point pour α^3 , 0,5 point pour l'égalité des corps, 0,5 point pour le polynôme minimal.

Erreur fréquente : affirmer que P est le polynôme minimal sans avoir prouvé qu'il est irréductible ou que α est de degré 4.

Exercice 3 : Corps de décomposition de $X^3 - 2$ (3 points)

a. Le critère d'Eisenstein s'applique avec $p = 2$: 2 divise 0, 0 et -2 , ne divise pas 1, et 4 ne divise pas 2. **Donc $X^3 - 2$ est irréductible sur $\mathbb{Q}$.** Ses racines sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, car $j^3 = 1$.

b. Le corps K est engendré par les trois racines. Il contient $\sqrt[3]{2}$ et $j = \frac{j\sqrt[3]{2}}{\sqrt[3]{2}}$, donc $\mathbb{Q}(\sqrt[3]{2}, j) \subset K$. Inversement, les trois racines sont dans $\mathbb{Q}(\sqrt[3]{2}, j)$. Donc $K = \mathbb{Q}(\sqrt[3]{2}, j)$.

D'abord, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, car $X^3 - 2$ est irréductible. Ensuite, j est racine de $X^2 + X + 1$, mais $j \notin \mathbb{Q}(\sqrt[3]{2})$, car ce corps est contenu dans $\mathbb{R}$. Le degré de j sur $\mathbb{Q}(\sqrt[3]{2})$ est donc 2.

Par la base télescopique, $[K : \mathbb{Q}] = 3 \times 2 = 6$.

- c. Le corps $\mathbb{Q}(\sqrt[3]{2})$ est inclus dans $\mathbb{R}$, alors que $j\sqrt[3]{2}$ n'est pas réel. **Les deux corps sont donc distincts**, bien qu'ils soient tous deux de degré 3 sur $\mathbb{Q}$.

Barème : a) 0,5 point pour l'irréductibilité, 0,5 point pour les racines ; b) 0,5 point pour l'égalité des corps, 1 point pour le degré 6 ; c) 0,5 point.

Exercice 4 : Corps finis F4 et F8, cyclicité du groupe multiplicatif (5 points)

- a. Le polynôme $X^2 + X + 1$ vaut 1 en 0 et en 1. De degré 2 sans racine, il est irréductible sur $\mathbb{F}_2$. Le quotient est donc un corps à $2^2 = 4$ éléments : $\mathbb{F}_4 = \{0, 1, \omega, \omega + 1\}$, avec $\omega^2 = \omega + 1$ (en caractéristique 2).

Table d'addition :

+	0	1	ω	$\omega + 1$
0	0	1	ω	$\omega + 1$
1	1	0	$\omega + 1$	ω
ω	ω	$\omega + 1$	0	1
$\omega + 1$	$\omega + 1$	ω	1	0

Table de multiplication, où $\omega(\omega + 1) = \omega^2 + \omega = 1$ et $(\omega + 1)^2 = \omega^2 + 1 = \omega$:

$\times$	1	ω	$\omega + 1$
1	1	ω	$\omega + 1$
ω	ω	$\omega + 1$	1
$\omega + 1$	$\omega + 1$	1	ω

b. On utilise la relation $\beta^3 = \beta + 1$ (en caractéristique 2). On obtient successivement :

$$\beta^0 = 1, \quad \beta^1 = \beta, \quad \beta^2 = \beta^2, \quad \beta^3 = \beta + 1;$$

$$\beta^4 = \beta^2 + \beta;$$

$$\beta^5 = \beta^3 + \beta^2 = \beta^2 + \beta + 1;$$

$$\beta^6 = \beta^3 + \beta^2 + \beta = \beta^2 + 1;$$

$$\beta^7 = \beta^3 + \beta = 1.$$

Les puissances $\beta^0, \dots, \beta^6$ sont les 7 éléments non nuls de $\mathbb{F}_8$, tous distincts. **Donc β est d'ordre 7 et engendre $\mathbb{F}_8^*$.** On pouvait aussi remarquer que 7 est premier et que $\beta \neq 1$.

c. Posons $n = q - 1 = |\mathbb{F}^*|$. Pour un diviseur d de n , notons $N(d)$ le nombre d'éléments d'ordre d dans $\mathbb{F}^*$.

Supposons $N(d) \geq 1$, et soit x d'ordre d . Les d éléments $1, x, \dots, x^{d-1}$ sont distincts et racines de $X^d - 1$. Or ce polynôme a au plus d racines dans le corps $\mathbb{F}$. Donc tout élément d'ordre d appartient à $\langle x \rangle$, qui est cyclique d'ordre d . Il en contient exactement $\varphi(d)$. Ainsi $N(d) \in \{0, \varphi(d)\}$.

Par le théorème de Lagrange, l'ordre de tout élément divise n . On a donc

$$n = \sum_{d|n} N(d) \leq \sum_{d|n} \varphi(d) = n. \text{ Toutes les inégalités sont des égalités, et en particulier } N(n) = \varphi(n) \geq 1. \text{ Donc } \mathbb{F}^* \text{ est cyclique.}$$

Dans $\mathbb{F}_{13}^*$, d'ordre 12, testons 2. Les diviseurs stricts maximaux de 12 sont 4 et 6. Or $2^4 = 16 \equiv 3$ et $2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$. Aucun ne vaut 1, donc 2 est d'ordre 12. Ainsi 2 engendre $\mathbb{F}_{13}^*$.

Barème : a) 0,5 point pour l'irréductibilité, 1 point pour les tables ; b) 1 point pour les puissances, 0,5 point pour la conclusion ; c) 1,5 point pour la démonstration ($N(d)$ au plus $\phi(d)$, sommation), 0,5 point pour le générateur de $\mathbb{F}_{13}^*$.

Exercice 5 : Problème : la duplication du cube et la trisection (4 points)

- a. Par la base télescopique appliquée à chaque étage, $[K_m : \mathbb{Q}] = 2^m$. Comme $\mathbb{Q} \subset \mathbb{Q}(x) \subset K_m$, le théorème de la base télescopique donne $[K_m : \mathbb{Q}] = [K_m : \mathbb{Q}(x)] [\mathbb{Q}(x) : \mathbb{Q}]$. Le degré $[\mathbb{Q}(x) : \mathbb{Q}]$ divise donc 2^m . **C'est une puissance de 2.**
- b. L'arête cherchée vérifie $a^3 = 2$, donc $a = \sqrt[3]{2}$. Son polynôme minimal est $X^3 - 2$, irréductible d'après l'exercice 3. Ainsi $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, qui n'est pas une puissance de 2. **La duplication du cube est impossible à la règle et au compas.**
- c. Avec $\theta = \frac{\pi}{9}$, on a $\cos(3\theta) = \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$. Donc $4c^3 - 3c = \frac{1}{2}$, soit $8c^3 - 6c = 1$. Comme $x = 2c$, cela s'écrit $x^3 - 3x - 1 = 0$.

Une racine rationnelle d'un polynôme unitaire à coefficients entiers est un entier qui divise le terme constant, donc ± 1 . Or $1 - 3 - 1 = -3$ et $-1 + 3 - 1 = 1$. Le polynôme $X^3 - 3X - 1$, de degré 3 sans racine rationnelle, est donc irréductible sur $\mathbb{Q}$. Ainsi $[\mathbb{Q}(x) : \mathbb{Q}] = 3$: **x n'est pas constructible**, et c non plus.

Or l'angle de 60° est constructible, grâce au triangle équilatéral. Si l'on savait le partager en trois, on construirait l'angle $20^\circ = \frac{\pi}{9}$, donc son cosinus c . **La trisection de l'angle de 60° est donc impossible à la règle et au compas.**

Barème : a) 1,5 point (degré de la tour, divisibilité) ; b) 1 point ; c) 0,5 point pour l'équation, 0,5 point pour l'irréductibilité, 0,5 point pour la conclusion sur la trisection.

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : extensions de corps et corps finis

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Corps et extensions](#) » en L3 puis entraînez-vous avec les **exercices corrigés** [corps et extensions](#).

Retrouvez tous les [contrôles de maths de L3 classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).

Autres contrôles de maths de L3 sur ce thème

- [Contrôle de maths L3 : partiel d'algèbre : groupes, anneaux et corps](#)