L3 MATH
2016-2017

Algèbre II
Contrôle du 8 février 2017
durée : 60 minutes

Les documents, calculatrices et téléphones portables sont interdits durant l'épreuve.
Les réponses doivent être justifiées.

Exercice 1

(1) Montrer que le nombre réel

$$\alpha = \frac{\sqrt[4]{111}}{\sqrt[3]{5} + \sqrt{468 - \sqrt{7}}}$$

est algébrique sur $\mathbb{Q}(i)$.

(2) Déterminer le polynôme minimal sur $\mathbb{Q}$ de

$$\beta = \sqrt[5]{7}e^{\frac{6\pi i}{5}}.$$

(3) Posons $\gamma = i\sqrt{2} + \sqrt{3}$.
   (a) Donner un polynôme annulateur de γ dans $\mathbb{Q}[X] \setminus \{0\}$.
   (b) Montrer que $\sqrt{3} \in \mathbb{Q}(\gamma)$.
   (c) Montrer que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$.
   (d) Déterminer le polynôme minimal de γ sur $\mathbb{Q}$.

(1) L'ensemble des nombres complexes algébriques est un corps, donc α est algébrique sur $\mathbb{Q}$ comme quotient de sommes de nombres algébriques. A fortiori, α est algébrique sur $\mathbb{Q}(i)$.

(2) $\beta = \sqrt[5]{7}e^{\frac{6\pi i}{5}}$, donc $\beta^5 = 7$. D'après le critère d'Eisenstein avec $p = 7$, $X^5 - 7$ est irréductible sur $\mathbb{Q}$. Comme il est de plus unitaire, c'est le polynôme minimal de β.

(3) (a) $\gamma = i\sqrt{2} + \sqrt{3}$, donc $(\gamma - \sqrt{3})^2 = -2$, d'où $\gamma^2 + 5 = 2\gamma\sqrt{3}$. En prenant le carré, $\gamma^4 - 2\gamma^2 + 25 = 0$. Le polynôme $X^4 - 2X^2 + 25$ est un polynôme annulateur de γ.

(b) Comme $(\gamma - \sqrt{3})^2 = -2$, $\sqrt{3} = (2\gamma)^{-1}(\gamma^2 + 5) \in \mathbb{Q}(\gamma)$.

(c) Montrons que γ est de degré 4. On sait déjà qu'il est de degré inférieur ou égal à 4 d'après 3a. Le corps $\mathbb{Q}(\gamma)$ est une extension de $\mathbb{Q}(\sqrt{3})$ d'après la question 3b, donc grâce au théorème de la base télescopique,

$$[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\gamma) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\gamma) : \mathbb{Q}(\sqrt{3})] \times 2.$$

Comme $i\sqrt{2} = \gamma - \sqrt{3}$ appartient à $\mathbb{Q}(\gamma)$ mais pas à $\mathbb{Q}(\sqrt{3})$ (qui est inclus dans $\mathbb{R}$), on a $[\mathbb{Q}(\gamma) : \mathbb{Q}(\sqrt{3})] \geqslant 2$, d'où $[\mathbb{Q}(\gamma) : \mathbb{Q}] \geqslant 4$.
Finalement, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$

(d) Le polynôme minimal de γ sur $\mathbb{Q}$ est de degré 4 d'après la question 3c et c'est un diviseur de $X^4 - 2X^2 + 25$ d'après la question 3a. Comme il de plus unitaire, il est égal à $X^4 - 2X^2 + 25$.

Exercice 2

Le but de cet exercice est de démontrer le résultat suivant :

Pour tout corps E tel que $\mathbb{Q} \subset E \subset \mathbb{C}$ et $[E : \mathbb{Q}] = d$ est fini, il existe un nombre algébrique γ tel que $E = \mathbb{Q}(\gamma)$.

On va procéder par récurrence sur d.

(1) Cas $d = 1$: montrer que si E est un corps tel que $\mathbb{Q} \subset E \subset \mathbb{C}$ et $[E : \mathbb{Q}] = 1$, le résultat est vrai.

Soit d un nombre entier, $d \geqslant 2$. Supposons le résultat vrai pour tous les corps contenant $\mathbb{Q}$ et de degré inférieur ou égal à $(d-1)$.

Soit E un corps tel que $\mathbb{Q} \subset E \subset \mathbb{C}$ et $[E : \mathbb{Q}] = d$.

(2) Soit $(e_1, \ldots, e_d)$ une base de E vu comme un $\mathbb{Q}$-espace vectoriel.
   (a) Montrer que pour tout $i \in \{1, \ldots, d\}$, e_i est algébrique sur $\mathbb{Q}$.
   (b) Montrer que $E = \mathbb{Q}(e_1, \ldots, e_d)$.

(3) Soient $\alpha, \beta \in \mathbb{C}$ deux nombres algébriques sur $\mathbb{Q}$.
   (a) Considérons les sous-corps de $\mathbb{Q}(\alpha, \beta)$

$$K_1 = \mathbb{Q}(\alpha + n_1\beta) \text{ et } K_2 = \mathbb{Q}(\alpha + n_2\beta)$$

   où $n_1, n_2 \in \mathbb{Z}$. Supposons qu'ils sont contenus *strictement* dans $\mathbb{Q}(\alpha, \beta)$. Montrer que $K_1 = K_2$ si et seulement si $n_1 = n_2$.
   (b) On admet que le corps $\mathbb{Q}(\alpha, \beta)$ n'admet qu'un nombre fini de sous-corps. Montrer qu'il existe $m \in \mathbb{Z}$ tel que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + m\beta)$.

(4) Conclure.

---

(1) Le corps E alors une extension de degré 1 de $\mathbb{Q}$, donc est égal à $\mathbb{Q} = \mathbb{Q}(1)$.

(2) (a) Soit $i \in \{1, \ldots, d\}$, e_i. Alors $\mathbb{Q}(e_i) \subset E$, donc le degré de $\mathbb{Q}(e_i)$ est au plus d, donc e_i est algébrique sur $\mathbb{Q}$ (de degré inférieur ou égal à d).

   (b) E est un corps qui contient $\mathbb{Q}$ et $e_1, \ldots, e_d$, donc il contient $\mathbb{Q}(e_1, \ldots, e_d)$ qui est le plus petit corps satisfaisant cette propriété. Réciproquement, si $x \in E$ alors comme $(e_1, \ldots, e_d)$ est une $\mathbb{Q}$-base de E, x peut s'écrire $x = \sum_{k=1}^{d} \lambda_k e_k$ avec $\lambda \in \mathbb{Q}$, donc $x \in \mathbb{Q}(e_1, \ldots, e_d)$.

(3) (a) Si $n_1 = n_2$, on a clairement $K_1 = K_2$.

   Supposons maintenant $K_1 = K_2 = K$ et supposons par l'absurde $n_1 \neq n_2$. Alors $\alpha + n_1\beta$ et $\alpha + n_1\beta$ sont dans K, donc leur différence $(n_1 - n_2)\beta \in K$. Comme K contient $\mathbb{Q}$ c'est un corps de caractéristique nulle, donc $(n_1 - n_2)$ est non nul donc inversible dans K, d'où $\beta \in K$. Par conséquent, $a \in K$ car $\alpha = (\alpha + n_1\beta) - n_1\beta$ est la somme de deux éléments de K. Donc K contient $\mathbb{Q}(\alpha, \beta)$, ce qui contredit l'hypothèse. D'où $n_1 = n_2$.

   (b) Considérons tous les corps $\mathbb{Q}(\alpha + m\beta)$, où m décrit $\mathbb{Z}$. S'ils sont tous distincts de $\mathbb{Q}(\alpha, \beta)$, on peut leur appliquer la question précédente : ils sont donc tous deux à deux distincts. Or c'est impossible puisqu'il n'existe qu'un nombre fini de sous-corps de $\mathbb{Q}(\alpha, \beta)$. Donc il existe $m \in \mathbb{Z}$ tel que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + m\beta)$ (c'est même vrai pour tout m sauf un nombre fini !).

(4) Notons, comme dans la question précédente, $(e_1, \ldots, e_d)$ une base de E comme $\mathbb{Q}$-espace vectoriel. Alors d'après la question 2b,

$$E = \mathbb{Q}(e_1, \ldots, e_d).$$

Posons $k = \min\{j \in \{1, \ldots, d\} \mid E = \mathbb{Q}(e_1, \ldots e_j)\}$. Si $k = 1$, alors $E = \mathbb{Q}(e_1)$ et on peut poser $\gamma = e_1$. Sinon,

$$E = (\mathbb{Q}(e_1, \ldots, e_{k-1}))(e_k) = E'(e_k),$$

en notant $E' = \mathbb{Q}(e_1, \ldots, e_{k-1})$.

Vérifions que nous pouvons appliquer l'hypothèse de récurrence à E'. D'après le théorème de la base télescopique, $d = [E : \mathbb{Q}] = [E : E'][E' : \mathbb{Q}]$. Or $[E : E'] > 1$ parce que $e_k \notin E'$ (par minimalité de k). Par hypothèse de récurrence, il existe donc δ algébrique tel que $E' = \mathbb{Q}(\delta)$, donc

$$E = \mathbb{Q}(\delta)(e_k) = \mathbb{Q}(\delta, e_k).$$

D'après la question (1)(b), il existe $m \in \mathbb{Z}$ tel que $\mathbb{Q}(\delta, e_k) = \mathbb{Q}(\delta + me_k)$. En posant $\gamma = \delta + me_k$, on a bien montré

$$E = \mathbb{Q}(\gamma).$$

On a bien démontré le résultat voulu, par récurrence sur le degré d de l'extension finie de $\mathbb{Q}$