Licence Pluridisciplinaire – Mathématiques
Corrigé de l'examen d'Algèbre – Deux heures
Seules les notes de cours et de travaux dirigés sont autorisées

Exercice 1 : la duplication du cube

On considère un cube $\mathcal{C} = ABCDEFGH$ dans l'espace affine euclidien usuel, de côté de longueur $AB = a > 0$. On se pose la question de savoir si l'on peut construire un cube $\mathcal{C}'$ à la règle et au compas dont le volume est le double de celui de $\mathcal{C}$.

1. Montrer que ce problème admet une solution si et seulement si $\sqrt[3]{2}$ est un nombre complexe constructible.

Solution. Puisque $\mathcal{C}'$ a un volume double de celui de $\mathcal{C}$, son volume est $2a^3$. Comme c'est un cube, la longueur de son côté est $\sqrt[3]{2}a$.

Pour construire un cube, il faut et il suffit de construire un côté. La longueur a étant donnée par hypothèse, il suffit de construire $\sqrt[3]{2}$ pour résoudre le problème. ■

2. Montrer que ce nombre n'est pas constructible. (On pourra considérer le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$.)

Solution. Le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est X^3-2 : il annule $\sqrt[3]{2}$ et il est irréductible sur $\mathbb{Q}$ puisqu'il n'a pas de racine dans $\mathbb{Q}$ (les racines sont $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{2\pi i}{3}}$, $\sqrt[3]{2}e^{-\frac{2\pi i}{3}}$). Donc

$$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = \deg(X^3 - 2) = 3,$$

qui n'est pas une puissance de 2. D'où le résultat. ■

Exercice 2 : racines de polynôme et extensions de $\mathbb{Q}$

Soit $P = X^6 + X^5 - X^3 - 3X^2 - 2X - 2$.

1. Effectuer la division euclidienne de P par $X^2 + X + 1$ et montrer que le quotient est $Q = X^4 - X^2 - 2$. Quel est le reste ?

Solution. On effectue la division selon les puissances décroissantes et on trouve le résultat énoncé. Le reste est nul. ■

2. Factoriser dans $\mathbb{C}$ le polynôme X^2+X+1. On note j la racine dont la partie imaginaire est strictement positive. Indiquer pourquoi j est constructible à la règle et au compas.

Solution. $X^2 + X + 1 = (X - j)(X - \bar{j})$ avec $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et $\bar{\jmath} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Le nombre j (et donc auss $\bar{j}$) est constructible car $\sqrt{3}$ est constructible. ■

3. Factoriser $Q = X^4 - X^2 - 2$ en facteurs irréductibles sur $\mathbb{C}$ puis sur $\mathbb{R}$ (On pourra remarquer que $Q \in \mathbb{Z}[X^2]$). En déduire la décomposition de Q en facteurs irréductibles sur $\mathbb{Q}$.

Solution. $X^4 - X^2 - 2 = Y^2 - Y - 2 = (Y-2)(Y+1)$ avec $Y = X^2$. On en déduit

$$X^4 - X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i),$$

ce qui est la décomposition en facteurs irréductibles sur $\mathbb{C}$. En regroupant racines complexes conjuguées, on trouve

$$X^4 - X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})(X^2 + 1),$$

ce qui est la décomposition en facteurs irréductibles sur $\mathbb{R}$. (Si $X^4 - X^2 - 2$ se décomposait davantage sur $\mathbb{R}$, alors la décomposition obtenue, par unicité, devrait coïncider avec celle sur $\mathbb{C}$, ce qui est impossible, puisque les racines autres que $\pm\sqrt{2}$ sont complexes non réelles.) La décomposition sur $\mathbb{Q}$ est

$$X^4 - X^2 - 2 = (X^2 - 2)(X^2 + 1).$$

(Si $X^4 - X^2 - 2$ se décomposait davantage sur $\mathbb{Q}$ alors la décomposition obtenue, par unicité, devrait coïncider avec celle sur $\mathbb{R}$, ce qui est impossible car $\sqrt{2} \notin \mathbb{Q}$.) ■

4. En déduire la décomposition de P en facteurs irréductibles sur $\mathbb{C}$ puis sur $\mathbb{R}$.

Solution. La décomposition sur $\mathbb{C}$ est

$$P(X) = (X - i)(X + i)(X - j)(X - \bar{j})(X - \sqrt{2})(X + \sqrt{2}).$$

La décomposition sur $\mathbb{R}$ est

$$P(X) = (X^2 + 1)(X^2 + X + 1)(X - \sqrt{2})(X + \sqrt{2}).$$

La première décomposition est la décomposition en facteurs irréductibles puisqu'ils sont tous de degré 1 ; la seconde vient du fait que les racines $\pm i, j, \bar{j}$ sont complexes non réelles. ■

5. Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{Q}$. En déduire la décomposition de P en facteurs irréductibles sur $\mathbb{Q}$.

Solution. Les racines $j, \bar{j}$ de $X^2 + X + 1$ ne sont pas rationnelles puisque $\sqrt{3} \notin \mathbb{Q}$. Donc $X^2 + X + 1$ est irréductible sur $\mathbb{Q}$. La décomposition en facteurs irréductibles de P sur $\mathbb{Q}$ est donc

$$P(X) = (X^2 + X + 1)(X^2 + 1)(X^2 - 2).$$

6. Soit $\gamma = \sqrt{2} + i \in \mathbb{C}$.

6.1. Montrer que $\mathbb{Q}[\gamma]$ est une extension de $\mathbb{Q}$.

Solution. γ est la somme de deux nombres algébriques et donc est lui-même algébrique. Donc $\mathbb{Q}[\gamma]$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$; c'est donc une extension de $\mathbb{Q}$. ■

6.2. Montrer que le polynôme minimal de γ sur $\mathbb{Q}$ est $X^4 - 2X^2 + 9$. (On pourra utiliser le fait que ses racines sont $\pm\gamma, \pm\bar{\gamma}$.)

Solution. On vérifie que ce polynôme admet γ comme racine. Montrons qu'il est irréductible sur $\mathbb{Q}$. La décomposition en facteurs irréductibles sur $\mathbb{C}$ est

$$X^4 - 2X^2 + 9 = (X - \gamma)(X - \bar{\gamma})(X + \gamma)(X + \bar{\gamma}).$$

Les racines étant complexes non réelles deux à deux conjuguées, la décomposition en facteurs irréductibles sur $\mathbb{R}$ est

$$X^4 - 2X^2 + 9 = (X^2 - 2\sqrt{2}X + 3)(X^2 + 2\sqrt{2}X + 3).$$

Si le polynôme $X^4 - 2X^2 + 9$ se décompose sur $\mathbb{Q}$, il admet au plus une décomposition en deux facteurs de degré deux (puisqu'aucune racine n'est rationnelle) ; par unicité de la décomposition sur $\mathbb{R}$, ce serait la même décomposition que sur $\mathbb{R}$, or les facteurs de cette décomposition sont à coefficients irrationnels. Donc $X^4 - 2X^2 + 9$ est irréductible sur $\mathbb{Q}$. C'est donc le polynôme minimal de γ sur $\mathbb{Q}$. ■

6.3. En déduire qu'une base de $\mathbb{Q}[\gamma]$ sur $\mathbb{Q}$ est $(1, \gamma, \gamma^2, \gamma^3)$. En déduire que $[\mathbb{Q}[\gamma] : \mathbb{Q}] = 4$.

Solution. Nous avons $\gamma^4 - 2\gamma^2 + 9 = 0$. On en déduit que $\gamma^4 = 2\gamma^2 - 9$ puis par une récurrence aisée que toute puissance de γ s'écrit comme une combinaison rationnelle (entière en fait) de $1, \gamma, \gamma^2$ et γ^3. Donc la famille $(1, \gamma, \gamma^2, \gamma^3)$ est génératrice. Considérons une relation rationnelle entre $1, \gamma, \gamma^2, \gamma^3$ qui est nulle : $a+b\gamma+c\gamma^2+d\gamma^3 = 0$. Il y a donc un polynôme R de degré ≤ 3 à coefficients dans $\mathbb{Q}$ qui s'annule sur γ. Or le polynôme minimal de γ est de degré 4. C'est donc que $R = 0$. On en déduit que le degré de l'extension est 4. ■

6.4. Montrer que $\mathbb{Q}[\gamma] = \mathbb{Q}[i, \sqrt{2}]$. Montrer qu'une base de $\mathbb{Q}[i, \sqrt{2}]$ sur $\mathbb{Q}$ est $(1, \sqrt{2}, i, i\sqrt{2})$. Écrire la matrice de passage de cette base à la base de la question 6.3.

Solution. L'inclusion $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[i, \sqrt{2}]$ est évidente. Pour voir la réciproque, $\mathbb{Q}[i, \sqrt{2}]$ et $\mathbb{Q}[\gamma]$ sont deux extensions de $\mathbb{Q}$ de degré 4. Par conséquent (deux espaces vectoriels de même dimension dont l'un est inclus dans l'autre sont égaux), elles coïncident. Le fait que $(1, i, \sqrt{2}, i\sqrt{2})$ est une base de $\mathbb{Q}[i, \sqrt{2}]$ a été vu en cours : "transitivité" des bases (et des degrés).

Calcul de la matrice de passage : on écrit les puissances de γ dans la base $(1, \sqrt{2}, i, i\sqrt{2})$.

$$\begin{bmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & -1 & 5 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \sqrt{2} \\ i \\ i\sqrt{2} \end{bmatrix}$$

On en déduit :

$$\begin{bmatrix} 1 \\ \sqrt{2} \\ i \\ i\sqrt{2} \end{bmatrix} = \frac{1}{6} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ -3 & 0 & 3 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \end{bmatrix}$$

Note. Les questions de 7 à 9 avaient été incluses dans une version antérieure du sujet de l'examen et ne figuraient pas dans le sujet de l'examen. Elles sont données ci-dessous avec leur corrigé à titre indicatif.

7. Soit $E = \mathbb{Q}[i, j, \sqrt{2}]$.

7.1. Montrer que E est une extension de $\mathbb{Q}[i, \sqrt{2}]$.

Solution. $E = \mathbb{Q}[i, \sqrt{2}][j] = \mathbb{Q}(i, \sqrt{2})[j]$. Puisque j est algébrique sur $\mathbb{Q}$, j est algébrique sur $\mathbb{Q}(i, \sqrt{2})$. Donc E est un corps. Comme E contient $\mathbb{Q}[i, \sqrt{2}]$, E est bien une extension de $\mathbb{Q}[i, \sqrt{2}]$. ■

7.2(*). On se propose de montrer que $\sqrt{3} \notin \mathbb{Q}[i, \sqrt{2}]$. On raisonne par l'absurde et on suppose que $\sqrt{3} = a + b\sqrt{2} + ci + di\sqrt{2} \in \mathbb{Q}[i, \sqrt{2}]$ avec $a, b, c, d \in \mathbb{Q}$. Élever au carré, écrire à nouveau dans la base $1, \sqrt{2}, i, i\sqrt{2}$ et identifier les coefficients.

Solution. En élevant au carré l'expression $\sqrt{3} = a + b\sqrt{2} + ci + di\sqrt{2}$, on trouve

$$3 = a^2 - b^2 + 2c^2 - 2d^2 + 2(ab + 2c)i + 2(ac - bd)\sqrt{2} + 2(ad + bc)i\sqrt{2}.$$

On en déduit le système

$$\left\{\begin{array}{rcl} a^2 - b^2 + 2c^2 - 2d^2 &=& 3 \\ ab + 2c &=& 0 \\ ac - bd &=& 0 \\ ad + bc &=& 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} a^2 - b^2 + 2c^2 - 2d^2 &=& 3 \\ c &=& -\frac{ab}{2} \\ b(a^2 + 2d) &=& 0 \\ a(2d - b^2) &=& 0 \end{array}\right.$$

On en déduit d'une part que $a = 0$ ou $b^2 = 2d$ et d'autre part que $b = 0$ ou $a^2 = -2d$.

Supposons d'abord $a = 0$: alors $c = -\frac{ab}{2} = 0$. Si $b = 0$ alors $d = 0$, ce qui conduit au quadruplet $(0, 0, 0, 0)$ qui n'est pas une solution. Si $b \neq 0$ alors $0 = a^2 = 2d$ donc $d = 0$, ce qui conduit à $b^2 = -3$, qui est impossible.

Supposons ensuite $b^2 = 2d$. Si $b = 0$ alors $d = 0$ et $c = 0$ donc $a^2 = 3$, ce qui est impossible. Si $b \neq 0$ alors $a^2 = -2d = -b^2$. Donc a^2 ou b^2 est négatif, ce qui est impossible.

L'examen des cas conduit à une contradiction dans tous les cas. Donc $\sqrt{3} \notin \mathbb{Q}[i, \sqrt{2}]$. ■

7.3. En déduire que $j \notin \mathbb{Q}[i, \sqrt{2}]$. En déduire que le polynôme minimal de j sur $\mathbb{Q}[i, \sqrt{2}]$ est $X^2 + X + 1$. En déduire que $[E : \mathbb{Q}[i, \sqrt{2}]] = 2$.

Solution. Si $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ était dans $\mathbb{Q}[i, \sqrt{2}]$, on en déduirait immédiatement que $\sqrt{3} \in \mathbb{Q}[i, \sqrt{2}]$, ce qui n'est pas d'après la question précédente. Donc le polynôme minimal S de j sur $\mathbb{Q}[i, \sqrt{2}]$ est au moins de degré 2. Or $X^2 + X + 1$ s'annule sur j, donc S est un multiple de $X^2 + X + 1$. Or $X^2 + X + 1$ est le polynôme minimal de j sur $\mathbb{Q}$ qui est nécessairement un multiple de S. Donc $S = X^2 + X + 1$. On en déduit que $[E : \mathbb{Q}[i, \sqrt{2}]] = 2$. ■

8. Montrer que $[E : \mathbb{Q}] = 8$.

Solution. D'après le théorème sur les degrés des extensions,

$$[E : \mathbb{Q}] = [E : \mathbb{Q}[i, \sqrt{2}]] \cdot [\mathbb{Q}[i, \sqrt{2}] : \mathbb{Q}] = 2 \cdot 4 = 8. ■$$

9. L'extension E est-elle contenue dans le corps $C(0, 1)$ des nombres complexes constructibles ? Justifier la réponse.

Solution. Puisque $C(0, 1)$ est une extension de $\mathbb{Q}$, il suffit de voir que $i, j, \sqrt{2} \in C(0, 1)$. On sait que $i \in C(0, 1)$ (cours) et que $C(0, 1)$ est stable par racine carrée : $2 \in C(0, 1)$ donc $\sqrt{2} \in C(0, 1)$; $3 \in C(0, 1)$ donc $\sqrt{3} \in C(0, 1)$ par conséquent $j \in C(0, 1)$. ■

Exercice 3 : extensions algébriques de degré arbitrairement grand

On se donne un entier $n \geq 2$. Soit $P_n = X^n - 2$.

1. Trouver les n racines complexes $z_0, \ldots, z_{n-1}$ de P_n. En déduire la décomposition de P en n facteurs irréductibles sur $\mathbb{C}$.

Solution. Les racines sont $z_k = \sqrt[n]{2}\exp(2\pi ik/n)$, $k = 0, 1, \ldots, n-1$. Elles sont simples et irrationnelles. La décomposition de P sur $\mathbb{C}$ est donc

$$X^n - 2 = \prod_{k=0}^{n-1}(X - z_k).\blacksquare$$

2. On considère une partie non vide $\mathcal{P} \subseteq \{z_0, \ldots, z_{n-1}\}$. Montrer que le polynôme

$$\prod_{z\in\mathcal{P}}(X - z)$$

est dans $\mathbb{Z}[X]$ si et seulement si $\mathcal{P} = \{z_0, \ldots, z_{n-1}\}$. (On pourra examiner le coefficient constant du polynôme.)

Solution. D'après la formule de la question précédente, la condition est suffisante. Réciproquement, supposons $\prod_{z\in\mathcal{P}}(X - z)$ dans $\mathbb{Z}[X]$. Donc le coefficient constant a_0 de ce polynôme doit être entier. Soit $1 \leq |\mathcal{P}| \leq n$ le cardinal de la partie $\mathcal{P}$.

$$a_0 = (-1)^{|\mathcal{P}|}\prod_{z\in\mathcal{P}} z \in \mathbb{Z}.$$

Puisque $|z| = \sqrt[n]{2}$ pour tout $z \in \mathcal{P}$,

$$|a_0| = \sqrt[n]{2}^{|\mathcal{P}|} = 2^{\frac{|\mathcal{P}|}{n}} \in \mathbb{Z}.$$

Ceci impose $|\mathcal{P}| = n$. Donc $\mathcal{P}$ est l'ensemble complet de toutes les racines de P_n. $\blacksquare$

3. En déduire que P_n est irréductible sur $\mathbb{Z}$, puis sur $\mathbb{Q}$.

Solution. Considérons une décomposition de P_n en facteurs irréductibles sur $\mathbb{Z}$. Au signe près, étant donnée la décomposition sur $\mathbb{C}$ (question 1), un des facteurs doit être de la forme $\prod_{z\in\mathcal{P}}(X-z)$ pour une certaine partie $\mathcal{P}$ non vide de $\{z_0, z_1, \ldots, z_{n-1}\}$. D'après la question précédente, ce facteur est à coefficients entiers si et seulement si $\mathcal{P} = \{z_0, z_1, \ldots, z_{n-1}\}$. Mais dans ce cas, le facteur est P_n lui-même. Donc P_n est irréductible sur $\mathbb{Z}$. Comme le coefficient dominant de P_n est 1, on en déduit que P_n est aussi irréductible sur $\mathbb{Q}$. $\blacksquare$

4. En déduire que pour tout entier $n \geq 2$, il existe un nombre algébrique z tel que $[\mathbb{Q}[z] : \mathbb{Q}] = n$.

Solution. Il suffit de choisir $z = \sqrt[n]{2}$. La question précédente montre que $P_n = X^n - 2$ est le polynôme minimal de z sur $\mathbb{Q}$. Donc l'extension $\mathbb{Q}[z]$ est de degré

$$[\mathbb{Q}[z] : \mathbb{Q}] = \deg(P_n) = n.\blacksquare$$