Nombres algébriques, nombres transcendants.

Dans tout le problème K est un sous-corps du corps des complexes $\mathbb{C}$ et $K[X]$ le K-espace vectoriel des polynômes sur K.

Pour tout $\alpha \in \mathbb{C}$, on note $K[\alpha]$ le K-espace vectoriel engendré par la famille $1, \alpha, \ldots, \alpha^q, \ldots$:

$$K[\alpha] = \{x \in \mathbb{C} \,|\, \mathrm{x}= \sum_{p=0}^{q} x_p \alpha^p,\ q \in \mathbb{N},\ x_0 \ldots x_q \in K\}.$$

Il est admis que l'ensemble $K[\alpha]$ est, pour la somme et le produit, un anneau.

Par définition, un nombre complexe α est *algébrique sur le corps* K si et seulement si il est racine d'un polynôme P, autre que le polynôme nul, appartenant à $K[X]$. Dans le cas contraire, le nombre α est *transcendant sur le corps* K.

Le but de ce problème est d'établir des propriétés simples des nombres algébriques et transcendants sur un corps K, d'en donner des exemples lorsque le corps K est celui des rationnels puis d'appliquer les résultats obtenus pour caractériser des figures géométriques constructibles « à la règle et au compas ».

Partie I

Dans cette partie, $K = \mathbb{Q}$ le corps des rationnels.

I-1) Exemples de nombres algébriques:

a) Montrer que $\sqrt{2}$ et $\sqrt{3}$ sont algébriques sur $\mathbb{Q}$. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un $\mathbb{Q}$-espace-vectoriel de dimension 2.

Dans la suite de cette question, on note $\alpha = \sqrt{2} + \sqrt{3}$.

b) Montrer que $\sqrt{6} \in \mathbb{Q}[\alpha]$, en déduire que α est algébrique sur $\mathbb{Q}$ et trouver un polynôme unitaire M_α de degré 4 à coefficients entiers dont α est racine.

c) Montrer que tout élément de $\mathbb{Q}[\alpha]$ s'écrit comme une combinaison linéaire à coefficients dans $\mathbb{Q}$ de 1, α, α^2 et α^3. Indication : utiliser une division euclidienne.

d) Montrer que le polynôme M_α n'a pas de racine dans $\mathbb{Q}$.

e) Montrer que $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. Montrer que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ forme une famille libre du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha]$, puis que c'en est une base.

f) Déduire de la question précédente que α n'annule pas de polynôme de degré inférieur ou égal 3 de $\mathbb{Q}[X]$ et que le polynôme M_α est irréductible dans $\mathbb{Q}[X]$.

g) On note f_α l'application de $\mathbb{Q}[\alpha]$ dans lui-même définie par $x \mapsto \alpha x$. Montrer que f_α est un endomorphisme, donner sa matrice dans la base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ puis calculer le polynôme caractéristique de cette matrice. Quel est le polynôme minimal de l'endomorphisme f_α ?

I-2) Entiers algébriques:

Un nombre complexe α est appelé *entier algébrique* si et seulement si il est racine d'un polynôme P non nul *unitaire à coefficients entiers.*

a) Montrer que $\sqrt{2} + \sqrt{3}$, $\frac{\sqrt{3}+\sqrt{7}}{2}$ et $\frac{1+i\sqrt{3}}{2}$ sont des entiers algébriques.

b) Montrer que $\frac{\sqrt{2}+\sqrt{3}}{2}$ est un nombre algébrique sur $\mathbb{Q}$ mais n'est pas un entier algébrique. Indication : utiliser le fait que $\sqrt{2} + \sqrt{3}$ n'annule pas de polynôme non nul de degré inférieur ou égal 3 à coefficient rationnel.

Partie II

Dans cette partie K est un sous-corps de $\mathbb{R}$ et α un *réel* algébrique sur le corps K; désignons par $\mathcal{I}(\alpha)$ l'ensemble des polynômes P appartenant à $K[X]$ qui admettent α comme racine:

$$\mathcal{I}(\alpha) = \{P | P \in K[X], P(\alpha) = 0\} .$$

II-1) $\mathcal{I}(\alpha)$ est un idéal de $K[X]$:

a) Démontrer que $\mathcal{I}(\alpha)$ est un idéal de $K[X]$. En déduire l'existence d'un polynôme M_α unitaire unique tel que $\mathcal{I}(\alpha)$ soit l'ensemble des polynômes de $K[X]$ proportionnels à M_α dans $K[X]$:

$$\mathcal{I}(\alpha) = \{P \ / \ \exists Q \in K[X],\ P = M_\alpha.Q\}.$$

b) Démontrer que, pour qu'un polynôme P, appartenant à $K[X]$, unitaire et irréductible dans $K[X]$, soit le polynôme M_α il faut et il suffit que le réel α soit racine du polynôme P.

Par définition le polynôme M_α est le *polynôme minimal* de α sur K, le degré du polynôme M_α, noté $d(\alpha, K)$, est le *degré* de α sur K.

II-2) Le degré de α sur K est égal à 1:

Le réel α et le corps K étant donnés, démontrer l'équivalence entre les affirmations suivantes:
i/ le réel α appartient à K, ii/ le degré de α sur K est égal à 1; iii/ $K[\alpha]$ est égal à K.

II-3) Dans cette question le degré de α sur K est égal à 2:

a) Préciser la dimension de $K[\alpha]$; démontrer que $K[\alpha]$ est un corps.

b) Démontrer qu'il existe un réel k ($k > 0$) appartenant au corps K tel que les deux corps $K[\alpha]$ et $K[\sqrt{k}]$ soient égaux.

Par définition, dans ce cas ($d(\alpha, K) = 2$), $K[\alpha]$ est *une extension quadratique* de K.

II-4) Dans cette question le degré de α sur K est égal à un entier $n \geqslant 2$:

a) Démontrer qu'à tout réel x appartenant à l'espace vectoriel $K[\alpha]$ est associé de manière unique un polynôme R de degré inférieur ou égal à $n-1$ appartenant à $K[X]$ tel que: $x = R(\alpha)$. En déduire une base du K-espace vectoriel $K[\alpha]$ et sa dimension.

b) Démontrer que, pour tout réel x (différent de 0) de $K[\alpha]$, le polynôme R ainsi associé est premier avec le polynôme minimal M_α. En déduire l'existence d'un polynôme U de $K[X]$ tel que la relation $U(\alpha).R(\alpha) = 1$ ait lieu.

c) Démontrer que l'anneau $K[\alpha]$ est un corps.

d) Démontrer que l'ensemble $K[\alpha]$ est le plus petit corps admettant α comme élément, contenant K et contenu dans $\mathbb{R}$ ($\alpha \in K[\alpha], K \subset K[\alpha] \subset \mathbb{R}$).

Le corps K est maintenant le corps des rationnels $\mathbb{Q}$. Considérons la suite des polynômes définis, pour tout réel x et pour tout entier naturel n, par les relations:

$$P_0(x) = 1,\ P_1(x) = 2x + 1,\ P_{n+2}(x) = 2xP_{n+1}(x) - P_n(x) .$$

Soit Q_n le polynôme défini par la relation $Q_n(x) = P_n(\frac{x}{2})$.

II-5) Propriétés générales des polynômes P_n:

a) Déterminer le degré du polynôme P_n, $n \geqslant 0$; préciser le coefficient du terme de plus haut degré et le terme constant. Déterminer les polynômes: P_2, P_3, P_4. Démontrer que les coefficients des polynômes Q_n (pour $n \geqslant 0$) sont des entiers relatifs.

b) Démontrer que les seules racines rationnelles possibles du polynôme Q_n sont les entiers 1 et -1. Exprimer l'expression $Q_{n+3}(x) + xQ_n(x)$ en fonction du polynôme $Q_{n+1}(x)$. En déduire que les racines rationnelles éventuelles des polynômes Q_{n+3} et Q_n sont les mêmes. Préciser les polynômes P_n qui ont une racine rationnelle.

II-6) Racines du polynôme P_n:

Soit θ un réel donné compris strictement entre 0 et π ($0 < \theta < \pi$). Considérons la suite $(u_n)_{n \geqslant 0}$ définie par la donnée de u_0 et de u_1 et la relation de récurrence:

$$\text{pour tout entier naturel } n, \quad u_{n+2} = 2u_{n+1}\cos\theta - u_n\ .$$

a) Déterminer l'expression du terme général u_n de la suite ci-dessus en fonction des réels n, θ et de deux scalaires λ et μ déterminés par θ, u_0 et u_1.

b) Utiliser les résultats précédents pour exprimer le réel $v_n = P_n(\cos\theta)$ en fonction des réels n et θ. En déduire toutes les racines du polynôme P_n notées $x_{k,n}$, $1 \leqslant k \leqslant n$.

c) Démontrer que les trois nombres réels $\cos(\frac{2\pi}{5}), \cos(\frac{2\pi}{7})$ et $\cos(\frac{2\pi}{9})$ sont algébriques sur $\mathbb{Q}$. Déterminer leur polynôme minimal.

II-7) Dans cette question le réel α est le nombre algébrique sur $\mathbb{Q}$, $\cos(\frac{2\pi}{9})$:

a) Démontrer que la dimension de l'espace vectoriel $Q[\alpha]$ est 3 et qu'une de ses bases est $B = (1, \alpha, \alpha^2)$. Donner l'expression dans cette base des réels $\cos(\frac{4\pi}{9}), \cos(\frac{8\pi}{9})$.

b) Soit f un endomorphisme non nul de l'espace vectoriel $Q[\alpha]$; supposons que, pour tout couple de réels x et y appartenant à $Q[\alpha]$, la relation $f(x.y) = f(x).f(y)$ ait lieu.

Déterminer les différentes images possibles des réels 1 et α dans la base B. En déduire que l'ensemble de ces endomorphismes est, pour la loi de composition des endomorphismes, un groupe à trois éléments f_1, f_2, f_3. Déterminer les matrices associées à ces endomorphismes f_1, f_2, f_3 dans la base B.

II-8) Exemple de nombres transcendants sur $\mathbb{Q}$:

Soit S un polynôme, appartenant à $Q[X]$, de degré $n \geqslant 2$, irréductible sur $\mathbb{Q}$.

a) Démontrer qu'il existe un entier naturel C_S (différent de 0) tel que pour tout rationnel $r = \frac{p}{q}$ (le couple (p,q) appartenant à $\mathbb{Z} \in \mathbb{N}^*$) il vienne: $|S(r)| \geqslant \frac{1}{C_S q^n}$.

b) Supposons que le réel α soit une racine de S. Déduire du résultat précédent l'existence d'une constante K, strictement positive, telle que pour tout rationnel $r = \frac{p}{q}$ appartenant à l'intervalle $[\alpha - 1, \alpha + 1]$, l'inégalité $|\alpha - r| \geqslant \frac{K}{q^n}$ ait lieu.

c) Soit $(t_n)_{n\in\mathbb{N}}$ la suite des réels définis par la relation: $t_n = \sum_{k=0}^{n} 10^{-k!}$, $n \geqslant 0$.

Démontrer que la suite $(t_n)_{n\in\mathbb{N}}$ est convergente; soit t sa limite. Établir l'inégalité: $|t - t_n| \leqslant 2.10^{-(n+1)!}$. En déduire que le réel t est transcendant sur $\mathbb{Q}$.

Partie III

Le but de cette partie est d'appliquer les résultats précédents pour caractériser les points du plan qui peuvent être construits « à la règle et au compas ».

Soit P un plan affine euclidien orienté. Considérons un repère orthonormé Oxy et K un sous-corps du corps des réels $\mathbb{R}$; posons:

- $\mathcal{K}$ est l'ensemble des points du plan P dont chaque coordonnée appartient au corps K.
- $\mathcal{D}$ est l'ensemble des droites du plan P qui joignent deux points de $\mathcal{K}$.
- $\mathcal{C}$ est l'ensemble des cercles du plan P centrés en un point de $\mathcal{K}$ et de rayon égal à la distance de deux points de $\mathcal{K}$.

III-1) Intersection de droites et de cercles appartenant à D ou à C:

Démontrer les résultats suivants:

• Toute droite appartenant à $\mathcal{D}$ et tout cercle appartenant à $\mathcal{C}$ admettent au moins une équation cartésienne dont les coefficients sont dans K.

• Le point commun à deux droites sécantes de $\mathcal{D}$ appartient à $\mathcal{K}$.

• Un point commun à une droite de $\mathcal{D}$ et à un cercle de $\mathcal{C}$ est soit un point de l'ensemble $\mathcal{K}$, soit un point dont chaque coordonnée appartient à une extension quadratique de K.

Que dire d'un point commun à deux cercles de $\mathcal{C}$?

Points et réels constructibles:

i/ Soit E un ensemble fini de points du plan P. Considérons toutes les droites passant par deux points de E et tous les cercles centrés en un de ces points de rayon égal à la distance de deux points quelconques de E. Les points d'intersection de ces droites et cercles deux à deux sont dits « *points construits à partir de E à la règle et au compas* » ou brièvement « construits à partir de E ».

ii/ Considérons deux point O et I du plan P. Un point M du plan P est dit « *constructible* » à partir des points O et I s'il existe une suite finie de points $M_1, M_2, \dots, M_n = M$ telle que:

• M_1 soit construit à partir de l'ensemble des deux points O et I,

• M_i, pour $2 \leqslant i \leqslant n$, soit construit à partir de l'ensemble $\{O, I, M_1, M_2, \dots, M_{i-1}\}$.

iii/ Dans la suite seuls le point O et le point I de l'axe Ox sont donnés; l'abscisse du point I est égale à 1; tout point M « constructible à partir des points O et I »est dit brièvement « *constructible* ».

iv/ Un réel est dit « *constructible* »s'il est égal à l'abscisse d'un point constructible de l'axe Ox ou à l'ordonnée d'un point constructible de l'axe Oy.

III-2) Exemples de points construits et de points et réels constructibles:

Démontrer, en justifiant un dessin effectué à l'aide d'une règle et d'un compas, les propriétés suivantes:

a) Soit E un ensemble de trois points A, B, C du plan P tels que ces points sont deux à deux distincts et ne sont pas alignés. Démontrer que le quatrième sommet D du parallélogramme $ABCD$ est un « point construit »à partir de l'ensemble E.

En déduire que si A et Δ sont un point et une droite du plan P donnés, la droite parallèle à la droite Δ passant par A peut être construite « à la règle et au compas ».

b) • Démontrer que le point J symétrique du point I par rapport à O est constructible ainsi que le point K porté par l'axe Oy d'ordonnée égale à 1. Il est admis que tout point dont les coordonnées sont des entiers relatifs, est constructible.

• Soient α et β deux réels strictement positifs constructibles; démontrer que les réels $\alpha + \beta$, $\frac{\alpha}{\beta}$ et $\alpha.\beta$ sont constructibles.

• Soit α un réel strictement positif constructible; démontrer que $\sqrt{\alpha}$ est constructible (on pourra considérer le cercle dont un diamètre est le segment joignant le point J au point $A(\alpha, 0)$).

Une suite finie $(K_i)_{0 \leqslant i \leqslant n}$, de sous-corps du corps des réels est dite avoir la propriété (P) si les deux relations ci-dessous ont lieu:

$(P1)$ $\quad \mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \dots K_n$,

$(P2)$ $\quad$ Pour tout entier i, $1 \leqslant i \leqslant n$, le corps K_i est une extension quadratique du corps K_{i-1}.

III-3) Une condition nécessaire et suffisante de constructibilité:

a) Soit M un point constructible; démontrer qu'il existe une suite finie $(K_i)_{0 \leqslant i \leqslant n}$, de sous-corps du corps des réels $\mathbb{R}$ ayant la propriété (P) et telle que les coordonnées de M appartiennent au corps K_n.

b) Soit une suite finie $(K_i)_{0 \leqslant i \leqslant n}$ ayant la propriété (P); démontrer par récurrence que tous les points M du plan dont les coordonnées appartiennent au corps K_n sont constructibles.

III-4) Une condition nécessaire de constructibilité:

a) Soient F, G et H trois sous-corps du corps des réels $\mathbb{R}$ tels que les inclusions $F \subset G \subset H$ aient lieu. Faisons les hypothèses: G est un F-espace vectoriel, H un G-espace vectoriel, leurs dimensions sont finies et respectivement égales aux entiers q et r. Démontrer que H est un F-espace vectoriel de dimension finie. Préciser sa dimension.

b) Considérons une suite finie $(K_i)_{0\leqslant i\leqslant n}$ de sous-corps du corps des réels ayant la propriété (P); quelle est la dimension du $\mathbb{Q}$-espace vectoriel K_n ?

c) En déduire que, si le réel α est constructible, le degré $d(\alpha,\mathbb{Q})$ est une puissance de l'entier 2.

Note historique: Les Grecs furent embarrassés lorsque la Pythie leur demanda un autel deux fois plus grand dans le temple d'Apollon à Delphes; la racine cubique de 2 n'est pas constructible !

III-5) Polygones réguliers constructibles:

Considérons les polygones réguliers à n côtés ($3 \leqslant n \leqslant 10$) inscrits dans le cercle de centre O et de rayon 1. Désignons par $A_1, A_2, \dots, A_n$ leurs sommets. Supposons le premier sommet A_1 confondu avec le point I. L'abscisse du deuxième sommet A_2 est égale à $\cos(\frac{2\pi}{n})$.

Quels sont, parmi les polygones réguliers à n côtés ($3 \leqslant n \leqslant 10$) inscrits dans le cercle de centre O et de rayon 1, ceux qui sont constructibles ?