

Dans tout le problème, \mathbf{K} est un sous-corps du corps \mathbf{R} des réels, et $\mathbf{K}[X]$ est l'algèbre des polynômes à une indéterminée sur \mathbf{K} . Par définition, un réel α est dit *algébrique* sur \mathbf{K} si α est racine d'un polynôme non nul à coefficients dans \mathbf{K} . Dans le cas contraire, α est dit *transcendant* sur \mathbf{K} . Dans le cas où \mathbf{K} est le corps \mathbf{Q} des rationnels, on se contente généralement de parler de *nombre transcendant* (sans préciser sur quel corps).

Le but de ce problème est d'établir des propriétés simples des nombres algébriques et transcendants sur un corps \mathbf{K} , d'en donner des exemples lorsque \mathbf{K} est le corps \mathbf{Q} des rationnels, puis d'appliquer les résultats obtenus pour caractériser les points du plan constructibles "à la règle et au compas".

Partie I

Soit α un réel algébrique sur \mathbf{K} , sous-corps de \mathbf{R} . On désigne par $I(\alpha)$ l'ensemble des polynômes P de $\mathbf{K}[X]$ dont α est racine.

1. a. Démontrer que $I(\alpha)$ est un idéal de $\mathbf{K}[X]$. En déduire l'existence d'un polynôme unitaire unique π_α , tel que $I(\alpha)$ soit l'ensemble des polynômes multiples de π_α .

b. Démontrer que pour qu'un polynôme P , appartenant à $\mathbf{K}[X]$, unitaire et irréductible dans $\mathbf{K}[X]$, soit le polynôme π_α , il faut et il suffit que α soit racine de P .

Par définition, le polynôme π_α est le *polynôme minimal* de α sur \mathbf{K} . Le degré de ce polynôme sera noté $\deg(\alpha, \mathbf{K})$, et il sera dit *degré* de α sur \mathbf{K} .

On note désormais $\mathbf{K}[\alpha] = \{P(\alpha), P \in \mathbf{K}[X]\}$, et on admet, c'est évident, que $\mathbf{K}[\alpha]$ est un anneau pour l'addition et la multiplication usuelle des réels.

2. Le réel α et le corps \mathbf{K} étant donnés, prouver l'équivalence des trois assertions suivantes :

- i.* α est un élément de \mathbf{K} .
- ii.* le degré de α sur \mathbf{K} est égal à 1.
- iii.* $\mathbf{K}[\alpha]$ est égal à \mathbf{K} .

3. Dans cette question, le degré de α sur \mathbf{K} est égal à 2.

On dit dans ce cas que $\mathbf{K}[\alpha]$ est une *extension quadratique* de \mathbf{K} .

- a.** Préciser la dimension de $\mathbf{K}[\alpha]$, et prouver que c'est un corps.
- b.** Démontrer qu'il existe un élément positif k du corps \mathbf{K} tel que les deux corps $\mathbf{K}[\alpha]$ et $\mathbf{K}[\sqrt{k}]$ soient égaux.

4. Dans cette question, le degré de α sur \mathbf{K} est un entier n supérieur ou égal à 2.

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

b. Démontrer que pour tout réel x non nul de $\mathbf{K}[\alpha]$, le polynôme R ainsi associé est premier avec π_α . En déduire que l'anneau $\mathbf{K}[\alpha]$ est un corps.

c. Retrouver le résultat précédent en envisageant l'application de \mathbf{K} dans $\mathbf{K} : y \mapsto xy$.

d. Démontrer que $\mathbf{K}[\alpha]$ est le plus petit corps intermédiaire entre \mathbf{K} et \mathbf{R} qui contienne α .

Le corps \mathbf{K} est maintenant le corps \mathbf{Q} des rationnels. Considérons la suite des polynômes définis par :

$$P_0 = 1, P_1 = 2X + 1, \forall n \geq 0, P_{n+2} = 2XP_{n+1} - P_n.$$

Soit enfin Q_n le polynôme défini par $Q_n(X) = P_n\left(\frac{X}{2}\right)$.

5. Propriétés générales des polynômes P_n .

a. Donner le degré du polynôme P_n , préciser son coefficient dominant ainsi que son terme constant. Déterminer les polynômes P_n pour $n = 1, 2, 3$, et prouver que, pour tout n , les coefficients des polynômes Q_n sont des entiers relatifs.

b. Démontrer que les seules racines rationnelles possibles du polynôme Q_n sont les entiers 1 et -1 . Exprimer le polynôme $Q_{n+3} + XQ_n$ en fonction de Q_{n+1} . En déduire que les racines rationnelles éventuelles des polynômes Q_{n+3} et Q_n sont les mêmes. Préciser les polynômes P_n possédant une racine rationnelle.

6. Racines du polynôme P_n .

Soit θ un réel donné compris strictement entre 0 et π . Considérons la suite (u_n) définie par la donnée de u_0 et de u_1 et la relation de récurrence :

$$\forall n \geq 0, u_{n+2} = 2u_{n+1}\cos\theta - u_n.$$

a. Déterminer l'expression du terme général u_n de la suite définie ci-dessus.

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 $x_{k,n}$ ($1 \leq k \leq n$) du polynôme P_n .

c. Démontrer que les trois réels $\cos\left(\frac{2\pi}{5}\right)$, $\cos\left(\frac{2\pi}{7}\right)$ et $\cos\left(\frac{2\pi}{9}\right)$ sont algébriques sur \mathbf{Q} , et déterminer pour chacun son polynôme minimal.

7. Existence de nombres transcendants.

Il s'agit ici de donner un argument simple prouvant l'existence de nombres transcendants (sur \mathbf{Q}) ; cette preuve présente toutefois un léger inconvénient : elle aboutit à la conclusion que "presque tous" les réels sont transcendants, sans toutefois en exhiber un seul !

a. Prouver que les réels algébriques (sur \mathbf{Q}) sont les racines des polynômes non nuls de $\mathbf{Z}[X]$.

b. Pour tout polynôme non nul à coefficients entiers, on définit son "poids" comme étant égal à son degré plus la

somme des valeurs absolues de ses coefficients : si $P \in \mathbf{Z}[X]$, $P = \sum_{k=0}^{\deg P} a_k X^k \neq 0$, $v(P) = \deg P + \sum_{k=0}^{\deg P} |a_k|$.

Prouver que pour tout entier k , l'ensemble des polynômes de poids égal à k est fini.

c. Prouver que l'ensemble des réels algébriques est dénombrable.

d. Rappeler une preuve de la non-dénombrabilité de \mathbf{R} (qui permet alors de conclure aisément, grâce à la question c., à l'existence de nombres transcendants).

8. Un exemple explicite de nombre transcendant sur \mathbf{Q} .

Soit S un polynôme irréductible de $\mathbf{Q}[X]$, de degré n supérieur ou égal à 2.

a. Prouver que S ne saurait posséder de racine rationnelle. En déduire qu'il existe un entier naturel non nul C_S tel

que pour tout rationnel $r = \frac{p}{q}$ (p et q entiers, q positif), on ait $|S(r)| \geq \frac{1}{C_S q^n}$.

b. Soit α une racine de S . Déduire du résultat précédent, et avec l'aide de l'inégalité des accroissements finis, l'existence d'une constante strictement positive K telle que, pour tout rationnel $r = \frac{p}{q}$ appartenant à l'intervalle

$[\alpha - 1, \alpha + 1]$, on ait l'inégalité $|\alpha - r| \geq \frac{K}{q^n}$.

c. Soient les réels $L_n = \sum_{k=0}^n 10^{-k!}$, et $L = \sum_{k=0}^{+\infty} 10^{-k!}$ (L en l'honneur de Liouville, découvreur de ce nombre

transcendant). Prouver que L est irrationnel. Établir l'inégalité $|L - L_n| \leq 2.10^{-(n+1)!}$. En déduire la transcendance de L .

Partie II

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 \mathcal{P} le plan euclidien orienté. Considérons un repère orthonormé Oxy et \mathbf{K} un sous-corps de \mathbf{R} . On adopte les notations suivantes :

\mathcal{K} est l'ensemble des points du plan dont chaque coordonnée appartient à \mathbf{K} .

\mathcal{D} est l'ensemble des droites du plan qui joignent deux points de \mathcal{K} .

\mathcal{C} est l'ensemble des cercles du plan centrés en un point de \mathcal{K} et de rayon égal à la distance entre deux points de \mathcal{K} .

1. Intersection de droites et de cercles appartenant à \mathcal{D} ou \mathcal{C}

Démontrer les résultats suivants :

a. Toute droite de \mathcal{D} et tout cercle de \mathcal{C} admettent au moins une équation cartésienne dont les coefficients sont dans

\mathbf{K} .

- b. Le point commun à deux droites sécantes de \mathcal{D} appartient à \mathcal{K} .
- c. 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 les coordonnées appartiennent toutes deux à une même extension quadratique de \mathbf{K} .
- d. Que peut-on dire d'un point commun à deux cercles de \mathcal{C} ?

Points et réels constructibles

Soit \mathcal{F} un ensemble fini de points du plan \mathcal{P} . Considérons toutes les droites passant par deux points de \mathcal{F} , et tous les cercles centrés en un point de \mathcal{F} et de rayon égal à la distance de deux points quelconques de \mathcal{F} . Les points d'intersection de ces droites et cercles sont dits *points construits à partir de \mathcal{F} à la règle et au compas* ou plus brièvement *points construits à partir de \mathcal{F}* .

Considérons deux points O et I du plan \mathcal{P} . Un point M du plan sera 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 est construit à partir des deux points O et I ;

$\forall j \in \{2, 3, \dots, n\}, M_j$ est construit à partir de l'ensemble $\{O, I, M_1, \dots, M_{j-1}\}$

Dans la suite, seuls le point O et le point I seront donnés, I étant le point de coordonnées $(1,0)$. Un point M constructible à partir des points O et I sera simplement dit *constructible*.

Un réel est dit *constructible* si c'est l'abscisse ou l'ordonnée d'un point constructible.

2. Exemples de points construits et de points constructibles

Démontrer, en justifiant par un dessin effectué à la règle et au compas, les propriétés suivantes :

a. Soit \mathcal{F} un ensemble constitué de trois points A, B et C du plan \mathcal{P} , deux à deux distincts et non alignés. Démontrer que le quatrième sommet D du parallélogramme $ABCD$ est un "point construit" à partir de l'ensemble \mathcal{F} .

En déduire que si A et Δ sont un point et une droite donnés de \mathcal{P} , la parallèle à 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.

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

On admettra, à partir de là, que tous les points dont les coordonnées sont des entiers relatifs sont constructibles.

d. 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 les points J et $A(\alpha,0)$).

Une suite finie $(\mathbf{K}_i)_{0 \leq i \leq p}$ de sous-corps de \mathbf{R} est dite avoir la propriété "TEQ" (comme *tour d'extensions quadratiques*) si cette suite est croissante au sens de l'inclusion, si \mathbf{K}_0 est \mathbf{Q} , et si pour tout entier i , le corps \mathbf{K}_i est une extension quadratique du corps \mathbf{K}_{i-1} .

3. Une condition nécessaire et suffisante de constructibilité

- a. Soit M un point constructible. Démontrer qu'il existe une suite finie $(\mathbf{K}_i)_{0 \leq i \leq p}$ de sous-corps de \mathbf{R} ayant la propriété "TEQ" telle que les coordonnées de M soient éléments de \mathbf{K}_p .
- b. Soit une suite finie $(\mathbf{K}_i)_{0 \leq i \leq p}$ de sous-corps de \mathbf{R} ayant la propriété "TEQ". Démontrer par récurrence que les points du plan dont les coordonnées sont dans \mathbf{K}_p sont constructibles.

4. Une condition nécessaire de constructibilité

- a. Soient F, G et H trois sous-corps emboîtés du corps des réels. On suppose que G est un F -espace vectoriel de dimension finie p , et que H est un G -espace vectoriel de dimension finie q . Montrer que H est un F -espace vectoriel de dimension finie égale à pq .
- b. Soit une suite finie $(\mathbf{K}_i)_{0 \leq i \leq p}$ de sous-corps de \mathbf{R} ayant la propriété "TEQ". Quelle est la dimension du \mathbf{Q} -espace vectoriel \mathbf{K}_p ?
- c. En déduire que si le réel α est constructible, alors α est un nombre algébrique sur \mathbf{Q} , et $\deg(\alpha, \mathbf{Q})$ est une puissance de 2.

Note historique : en particulier, un nombre algébrique aussi simple que $\sqrt[3]{2}$ n'est donc pas constructible à la règle et au compas : cela explique l'embarras des Grecs lorsque la Pythie leur demanda un autel deux fois plus grand dans le temple d'Appolon à Delphes. Dans le même ordre d'idée, cela prouve aussi que le fameux problème de la quadrature du cercle posé par ces mêmes Grecs n'a pas de solution : en effet, construire un carré de même aire qu'un cercle donné revient à construire le nombre $\sqrt{\pi}$. Or, Ferdinand LINDEMANN a démontré en 1882 que π , et donc aussi $\sqrt{\pi}$, est transcendant, ce qui lui interdit d'être constructible...

5. La réciproque de la question précédente est inexacte

On se propose ici de prouver qu'il existe des réels de degré 4 sur \mathbf{Q} , et qui ne sont pas constructibles.

Envisageons le polynôme $P = X^4 - 4X + 2$.

- a. Prouver que P possède exactement deux racines réelles r_1 et r_2 , et que celles-ci sont irrationnelles.
- b. On factorise P dans $\mathbf{R}[X]$ sous la forme : $P = (X^2 + aX + b)(X^2 + cX + d)$.
Prouver que le réel $t = b + d$ est racine d'une équation du troisième degré que l'on explicitera.
Déterminer le degré de t sur \mathbf{Q} .
- c. Prouver que P est irréductible sur \mathbf{Q} , et en déduire le degré des r_i sur \mathbf{Q} .
- d. Démontrer que l'un au moins des deux réels r_1 et r_2 n'est pas constructible.

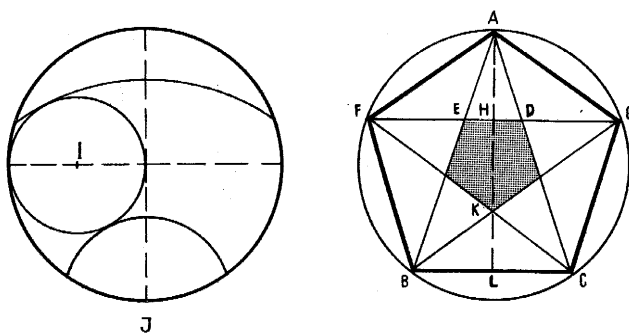
6. Polygones réguliers constructibles

Considérons les polygones réguliers à n côtés (n entier plus grand que 3) inscrits dans le cercle unité. Désignons par A_1, A_2, \dots, A_n leurs sommets. On supposera que le point A_1 est confondu avec le point I , et que A_2 est celui de ces points dont les coordonnées sont $\left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$.

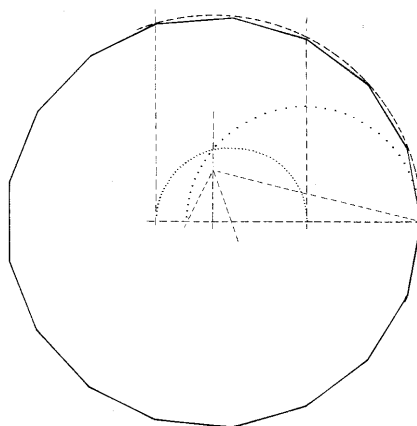
Quels sont, parmi les polygones réguliers à n côtés (pour $3 \leq n \leq 10$), ceux qui sont constructibles ?

Note historique (deuxième) : A la suite des travaux de Gauss qui, à dix-neuf ans, a prouvé la constructibilité du polygone régulier à 17 côtés, on a pu déterminer une condition nécessaire et suffisante pour que le polygone régulier à n côtés soit constructible : il faut et il suffit que n s'écrive $2^p F_1 F_2 \dots F_k$ où p et k sont des entiers quelconques, les F_i étant des nombres premiers de Fermat deux à deux distincts. Cela explique que le polygone à 17 côtés, mais aussi les polygones à 257 et 65537 côtés, soient constructibles (une construction de ce dernier existe ; elle est monstrueuse...)

Le pentagone régulier



L'heptadécagone régulier



Pour mieux voir, consulter : <http://www.ac-poitiers.fr/math/prof/resso/ima/sar1/>