I. Petite promenade dans $\mathbb{Z}/37\mathbb{Z}$

On travaille dans tout cet exercice dans l'anneau $\mathbb{Z}/37\mathbb{Z}$. On note U le groupe multiplicatif constitué de ses éléments inversibles. La classe d'un entier x dans $\mathbb{Z}/37\mathbb{Z}$ sera notée $\overline{x}$.

1. **a.** Prouver que $\mathbb{Z}/37\mathbb{Z}$ est un corps.

b. Combien U possède-t-il d'éléments ?

c. Quels sont les ordres possibles d'un élément de U ?

d. Déterminer l'ordre de $\overline{2}$ et prouver que U est monogène.

e. Déterminer l'ordre de $\overline{10}$.

2. **a.** Déterminer l'inverse de $\overline{8}$ dans $\mathbb{Z}/37\mathbb{Z}$.

b. Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ l'équation du troisième degré $x^3+\overline{1}=\overline{0}$ (*indication :* faites marcher votre mémoire à court terme !).

3. **a.** Quels sont les éléments de $\mathbb{Z}/37\mathbb{Z}$ qui sont égaux à leur propre inverse ?

b. En déduire que $36!\equiv -1\,[37]$.

4. **a.** Prouver que pour tout x non nul de $\mathbb{Z}/37\mathbb{Z}$, on a $x^{36}=\overline{1}$.

b. Prouver que l'on ne peut avoir $x^{18}=\overline{1}$ pour tout x non nul de $\mathbb{Z}/37\mathbb{Z}$ (on demande un argument théorique, indépendant des calculs effectués précédemment).

c. Retrouver le fait que U est un groupe monogène.

II. Irrationalité de π

On suppose ici l'existence de deux entiers positifs et premiers entre eux a et b tels que $\pi=\dfrac{a}{b}$.

Pour n entier naturel et x réel, on pose :

$$P_n(x)=\frac{x^n(a-bx)^n}{n!} \quad \text{et} \quad I_n=\int_0^\pi P_n(x)\sin x\,\mathrm{d}x\,.$$

5. **a.** Calculer $\sup\limits_{0\leq x\leq\pi}\left|P_n(x)\right|$ en fonction de a, b et n.

b. Prouver que I_n est strictement positif pour tout n, et déterminer la limite de la suite (I_n).

6. Pour tout entier k, la dérivée d'ordre k du polynôme P_n sera notée $P_n^{(k)}$. Par définition, $P_n^{(0)}=P_n$. Calculer en fonction de a, b, n et k les valeurs de $P_n^{(k)}(0)$ et de $P_n^{(k)}\left(\dfrac{a}{b}\right)$ dans les trois cas suivants :

i. $0\leq k\leq n-1$ (lorsque $n\geq 1$) ;

ii. $k\geq 2n+1$;

iii. $n\leq k\leq 2n$.

Montrer que dans tous les cas considérés, $P_n^{(k)}(0)$ et $P_n^{(k)}(\frac{a}{b})$ sont des entiers relatifs.

7. Montrer que I_n est un entier relatif.

b. Prouver que π est irrationnel.

III. Problème

L'objet de ce problème est, dans un premier temps (partie **1.**), de localiser dans le plan complexe les racines d'un polynôme donné (questions **8.** et **9.**). Quitte à le multiplier par une constante, ce polynôme sera supposé unitaire. Les questions **10.** et **11.** traitent des exemples. Elles peuvent être abordées sans avoir résolu les questions précédentes puisque la question **9.** explicite clairement les résultats qui sont utiles. Dans la partie **2.**, la question **12.** fournit un algorithme de détermination de la racine de plus grand module d'un polynôme complexe. Enfin, la partie **3.** explicite des polynômes dont trois réels donnés sont racines, en lien avec la constructibilité des polygones réguliers à 5, 7 et 9 côtés à la règle et au compas. Ce lien n'est cependant pas étudié ici.

Partie 1.

Soit $P = X^p + a_{p-1}X^{p-1} + \ldots + a_1X + a_0$ un polynôme complexe de degré p avec $p \geq 2$.

On notera $M = \max_{0\leq k\leq p-1}(|a_k|) = \max(|a_{p-1}|,\ldots,|a_1|,|a_0|)$.

8. On considère la fonction f définie sur $\mathbb{R}^+$ par $f(t) = t^{p+1} - (M+1)t^p + M$.

a. Déterminer l'unique zéro strictement positif α de la dérivée f' de f.

Comparer les positions respectives de α et de 1 en fonction des positions respectives de M et de $1/p$.

b. On suppose $M \leq 1/p$. Dresser le tableau de variations de f sur $\mathbb{R}^+$.

En déduire le signe de $f(t)$ pour $t > 1$.

c. On suppose $M > 1/p$. Dresser le tableau de variations de f sur $\mathbb{R}^+$.

En déduire le signe de $f(t)$ pour $t > M+1$.

9. **a.** Soit a une racine (réelle ou complexe) différente de 1 du polynôme P.

Montrer l'inégalité :

$$|a|^p \leq M\frac{|a|^p - 1}{|a| - 1}$$

En supposant $|a| > 1$, montrer alors que l'on a l'inégalité :

$$f(|a|) = |a|^{p+1} - (M+1)|a|^p + M \leq 0\,.$$

b. On suppose $M \leq 1/p$. Prouver alors que toutes les racines de P sont de module inférieur ou égal à 1.

c. On suppose $M > 1/p$. Prouver alors que toutes les racines de P sont de module strictement inférieur à $M+1$.

10. On prend dans cette question $P = X^p - \frac{1}{p}(X^{p-1} + \ldots + X + 1) = X^p - \frac{1}{p}\sum_{k=0}^{p-1} X^k$.

a. Montrer que les racines de P sont de module inférieur ou égal à 1.

b. Montrer que 1 est une racine simple de P. Qu'en déduit-on par rapport à la question **9.b.** ?

11. On prend dans cette question $P = X^p - (X^{p-1} + \ldots + X + 1) = X^p - \sum_{k=0}^{p-1} X^k$.

a. Montrer que les racines de P sont de module strictement inférieur à 2.

b. Prouver que si z est une racine de P, z est aussi une racine du polynôme $X^{p+1} - 2X^p + 1$.

c. En étudiant la fonction définie sur $\mathbb{R}^+$ par $g(t) = t^{p+1} - 2t^p + 1$, en déduire que P possède une racine réelle comprise entre $\dfrac{2p}{p+1}$ et 2. Qu'en déduit-on par rapport à la question **9.c.** ?

d. Prouver enfin que z est une racine de P si et seulement si $z' = 1/z$ est une racine de $Q = X^p + X^{p-1} + \ldots + X - 1$.

En déduire que toutes les racines de P sont de module compris entre $1/2$ et 2.

Partie 2.

12. On considère dans cette question un élément F de $\mathbb{C}[X]$, unitaire et de degré n, possédant dans $\mathbb{C}$ n racines $r_1, r_2, \ldots, r_n$ qui vérifient : $|r_1| \leq |r_2| \leq \ldots \leq |r_{n-1}| < |r_n|$.

a. Soit P un polynôme de $\mathbb{C}[X]$. Prouver que le polynôme Q défini par $Q(X) = P(X)P(-X)$ est un polynôme pair, et en déduire l'existence et l'unicité d'un polynôme P^* de $\mathbb{C}[X]$ tel que $P^*(X^2) = P(X)P(-X)$.

b. Calculer P^* quand P est le polynôme du second degré $P = X^2 + aX + b$.

b. Soit P un polynôme unitaire de $\mathbb{C}[X]$ se factorisant dans $\mathbb{C}[X]$ sous la forme $P(X) = \prod_{i=1}^{n} (X - x_i)$. Exprimer simplement P^*.

On considère la suite $(P_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{C}[X]$ définie par :

$$P_0 = F \quad \text{et pour tout entier } k,\ P_{k+1} = (-1)^n P_k{}^* .$$

On note par ailleurs α_k le coefficient de X^{n-1} dans P_k.

c. Donner une expression simple du polynôme P_k et déterminer ses racines en fonction de celles de F.

d. Exprimer α_k en fonction de k et des racines de F.

e. Déterminer $\lim\limits_{k\to+\infty} |\alpha_k|^{\frac{1}{2^k}}$.

Partie III

On construit par récurrence une suite (P_n) de polynômes de la façon suivante :

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

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

13. **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.

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 :

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

14. **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 $\cos(\frac{2\pi}{5})$, $\cos(\frac{2\pi}{7})$ et $\cos(\frac{2\pi}{9})$ sont racines de polynômes non nuls à coefficients entiers, et expliciter pour chacun un tel polynôme dont il est racine.