Devoir surveillé 1

Vendredi 20 septembre 2019
L'usage des calculatrices est interdit

Vous attacherez la plus grande importance à la clarté, à la précision et à la concision de la rédaction, même si tout résultat qui n'est pas explicitement dans le cours de MPSI ou de MP doit être démontré. Si vous repèrez ce qui semble être une erreur d'énoncé, signalez le sur votre copie et poursuivez votre composition en expliquant les raisons des initiatives que vous avez été amené à prendre.

EXERCICE 1 :

On travaille dans tout l'exercice dans l'anneau $\mathbb{Z}/37\mathbb{Z}$. On note U l'ensemble constitué de ses éléments inversibles. On note $\overline{x}$ la classe d'équivalence de x dans $\mathbb{Z}/37\mathbb{Z}$.

1. **a.** Rappeler la définition de la relation d'équivalence $\mathcal{R}$ définie dans $\mathbb{Z}$ permettant de construire $\mathbb{Z}/37\mathbb{Z}$.

b. Quelle est la classe d'équivalence de 4 ?

c. Donner la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/37\mathbb{Z}$. Vous montrerez que la multiplication est définie de manière cohérente.

2. **a.** Démontrer que $\mathbb{Z}/37\mathbb{Z}$ est un corps.

b. Quel est le cardinal de U ?

c. Démontrer que $(U, \cdot)$ est un groupe.

d. Quels sont les ordres possibles d'un élément de $(U, \cdot)$?

e. Déterminer la classe de 2^{18} (on pourra utiliser l'exponentiation rapide) puis déterminer l'ordre de $\overline{2}$ dans $(U, \cdot)$ et conclure que U est cyclique.

f. Déterminer l'ordre de $\overline{10}$ dans $(U, \cdot)$.

3. **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 $x^3 + 1 \equiv 0[37]$.

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

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

5. **a.** Énoncer puis démontrer le théorème d'Euler dans $\mathbb{Z}/n\mathbb{Z}$. Qu'obtient-on dans $\mathbb{Z}/37\mathbb{Z}$?

b. Justifier par un argument théorique indépendant des calculs précédents qu'il existe $\overline{x} \in \mathbb{Z}/37\mathbb{Z} \setminus \{\overline{0}\}$ tel que $x^{18} \neq 1[37]$.

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

PROBLEME :

Soit $n \in \mathbb{N}$. On admet l'existence d'un polynôme T_n tel que

$$\forall \theta \in \mathbb{R}, T_n(\cos\theta) = \cos(n\theta).$$

On admet l'existence d'un polynôme U_n tel que

$$\forall \theta \in \mathbb{R} \setminus \pi\mathbb{Z}, U_n(\cos\theta) = \frac{\sin((n+1)\theta)}{\sin\theta}.$$

Partie A

1. Justifier que si A et B sont deux polynômes tels que $\forall x \in]-1,1[, A(x) = B(x)$, alors $A = B$.
En déduire l'unicité des polynômes T_n et U_n.

2. Déterminer T_0, T_1, T_2, T_3.

3. En remarquant que pour tout réel θ, on a $\cos(n\theta) = Re\left((e^{i\theta})^n\right)$, montrer que

$$\forall n \in \mathbb{N}, T_n = \sum_{0 \leqslant k \leqslant n/2} \binom{n}{2k} (X^2-1)^k X^{n-2k}.$$

4. Montrer que la suite $(T_n)_{n\in\mathbb{N}}$ vérifie la relation de récurrence

$$\forall n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n.$$

5. En déduire pour tout entier naturel n le degré et le coefficient dominant de T_n.

6. Soit $n \in \mathbb{N}$. Pour quels $\theta \in \mathbb{R}$ a-t-on $\cos(n\theta) = 0$?
Montrer que pour tout entier naturel n, le polynôme T_n est scindé sur $\mathbb{R}$, à racines simples appartenant à $]-1,1[$.
Déterminer les racines de T_n.

7. Vérifier que pour tout $n \in \mathbb{N}, U_n = \dfrac{1}{n+1} T'_{n+1}$.

8. Montrer que la suite $(U_n)_{n\in\mathbb{N}}$ vérifie la même relation de récurrence que la suite $(T_n)_{n\in\mathbb{N}}$.

9. Pour tout entier naturel n, montrer que le polynôme U_n est scindé sur $\mathbb{R}$ à racines simples appartenant à $]-1,1[$ et determiner les racines de U_n.

Partie B :

1. Montrer que

$$\begin{cases} T_m \cdot T_n = \dfrac{1}{2}(T_{n+m} + T_{n-m}) & \text{pour tous entiers } 0 \leqslant m \leqslant n \\ T_m \cdot U_{n-1} = \dfrac{1}{2}(U_{n+m-1} + U_{n-m-1}) & \text{pour tous entiers } 0 \leqslant m < n \end{cases}$$

2. Pour m et n entiers naturels tels que $m \leqslant n$, on se propose de déterminer le quotient $Q_{n,m}$ et le reste $R_{n,m}$ de la division euclidienne de T_n par T_m.

- **a.** On suppose $m < n < 3m$. Montrer que $Q_{n,m} = 2T_{n-m}$ et que $R_{n,m} = -T_{|n-2m|}$ (on pourra étudier le cas où $2m \leqslant n < 3m$ puis le cas $m \leqslant n < 2m$).
- **b.** Déterminer $Q_{n,m}$ et $R_{n,m}$ lorsque $n = 3m$ puis lorsque n est de la forme $(2p+1)m$ avec $p \in \mathbb{N}^*$.
- **c.** On suppose que $m > 0$ et que n n'est pas le produit de m par un entier impair. Montrer qu'il existe un unique entier $p \geqslant 1$ tel que $|n - 2pm| < m$ puis montrer par récurrence sur p que :

$$Q_{n,m} = 2\left(T_{n-m} - T_{n-3m} + \cdots + (-1)^{p-1} T_{n-(2p-1)m}\right) \text{ et } R_{n,m} = (-1)^p T_{|n-2pm|}.$$

Partie C

On fixe deux entiers naturels m et n.

1. Soit h le pgcd dans $\mathbb{N}$ de $m+1$ et $n+1$. En examinant les racines communes à U_n et U_m, montrer que U_{h-1} est un pgcd de U_n et U_m dans $\mathbb{R}[X]$.

2. Soit $g > 0$ le pgcd de m et n. On pose $m_1 = m/g$ et $n_1 = n/g$.

a. Montrer que si m_1 et n_1 sont impairs, alors T_g est un pgcd de T_n et de T_m.

b. Montrer que si l'un des deux entiers m_1 ou n_1 est pair, alors T_n et T_m sont premiers entre eux.

c. Que peut-on dire des pgcd de T_n et T_m lorsque m et n sont impairs ? Lorsque n et m sont deux puissances de 2 distinctes ?

Partie D :

Dans cette partie, on munit l'ensemble $\mathbb{C}[X]$ des polynômes complexes de la loi de composition interne associative donnée par la composition, notée $\circ$. Plus précisément, étant donné P et Q dans $\mathbb{C}[X]$, si $P = \sum_{k=0}^{+\infty} p_k X^k$, pour une suite presque nulle (p_k), on a :

$$P \circ Q = \sum_{k=0}^{+\infty} p_k Q^k.$$

On dit que les polynômes P et Q commutent si $P \circ Q = Q \circ P$. On note $\mathcal{C}(P)$ l'ensemble des polynômes complexes qui commutent avec le polynôme P.

On cherche dans cette partie les familles $(F_n)_{n\in\mathbb{N}}$ de polynômes complexes vérifiant la propriété

$$(\mathbb{P}) : \forall n \in \mathbb{N}, deg(F_n) = n \text{ et } \forall (m,n) \in \mathbb{N}^2, F_n \circ F_m = F_m \circ F_n.$$

Il est clair que la famille $(X^n)_{n\in\mathbb{N}}$ convient.

On note G l'ensemble des polynômes complexes de degré 1 et pour $\alpha \in \mathbb{C}$, on pose $P_\alpha = X^2 + \alpha$.

1. Montrer que la familles $(T_n)_{n\in\mathbb{N}}$ vérifie la propriété $(\mathbb{P})$. On pourra comparer $T_n \circ T_m$ et T_{nm}.

2. Vérifier que G est un groupe pour la loi $\circ$.
L'inverse d'un élément U de G pour la loi $\circ$ sera noté U^{-1}.

3. Soit $\alpha \in \mathbb{C}$ et soit Q un polynôme complexe non constant qui commute avec P_α. Montrer que Q est unitaire.

4. En déduire que pour tout entier $n \geqslant 1$, il existe au plus un polynôme de degré n qui commute avec P_α. Déterminer $\mathcal{C}(X^2)$.

5. Soit P un polynôme complexe de degré 2. Justifier l'existence et l'unicité de $U \in G$ et $\alpha \in \mathbb{C}$ tels que $U \circ P \circ U^{-1} = P_\alpha$. Déterminer ces deux éléments lorsque $P = T_2$.

6. Justifier que $\mathcal{C}(T_2) = \{-1/2\} \cup \{T_n, n \in \mathbb{N}\}$.