Devoir surveillé

1 Les questions **1)** à **3)** suivantes sont indépendantes.

1) Pourquoi n'existe-t-il pas de polynôme $P \in \mathbb{C}[X]$ pour lequel $P(z) = \mathrm{Re}(z) + \mathrm{Im}(z)$ pour tout $z \in \mathbb{C}$?

2) On pose $P = (X+1)^7 - X^7 - 1$.

a) Déterminer le degré et deux racines entières de P, puis montrer que j en est racine.

b) Déterminer la forme scindée de P sur $\mathbb{C}$.

3) Résoudre l'équation polynomiale $(X-1)P' = 3P$ d'inconnue $P \in \mathbb{R}[X]$.

---

2 On s'intéresse dans ce problème à des couples de polynômes de $\mathbb{C}[X]$ qui commutent au sens de la composition. On rappelle que la composition est associative et que pour tous $P, Q \in \mathbb{C}[X]$, si Q n'est pas constant, alors $\deg(P \circ Q) = \deg(P).\deg(Q)$.

1) On note $\mathscr{U}$ l'ensemble des polynômes de degré 1 de $\mathbb{C}[X]$, puis on pose $\lambda(P) = a$ pour tout $P = aX + b \in \mathscr{U}$. Montrer que $\mathscr{U}$ est un groupe pour la composition et que λ est un morphisme de groupes de $\mathscr{U}$ dans $\mathbb{C}^*$.

On pose $\mathscr{C}_d(P) = \Big\{ Q \in \mathbb{C}[X] \mid \quad P \circ Q = Q \circ P \quad \text{et} \quad \deg(Q) = d \Big\}$ pour tous $P \in \mathbb{C}[X]$ et $d \in \mathbb{N}^*$.

2) Soit $P \in \mathbb{C}[X]$ de degré $n \geqslant 2$.

a) Montrer que $\mathscr{C}_1(P)$ est un sous-groupe de $\mathscr{U}$ et que pour tout $U \in \mathscr{C}_1(P)$: $\quad \lambda(U) \in \mathbb{U}_{n-1}$.

b) Montrer que le morphisme $\lambda_{|\mathscr{C}_1(P)}$ est injectif.

c) En déduire que $\big|\mathscr{C}_1(P)\big|$ divise $n-1$.

3) Soient $P, Q \in \mathbb{C}[X]$ deux polynômes de même degré $d \geqslant 1$ et de même coefficient dominant. Montrer que pour tout $n \in \mathbb{N}^*$: $\quad \deg\big(P^n - Q^n\big) = \deg(P-Q) + (n-1)d$.

Pour tout $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$, on dira dans les questions qui suivent que P est *réduit* si son coefficient de degré $n-1$ est nul.

En vue des questions **4)** et **5)**, on fixe un polynôme $P \in \mathbb{C}[X]$ de degré $n \geqslant 2$ à la fois unitaire et réduit et un entier $d \in \mathbb{N}^*$. On suppose $\mathscr{C}_d(P)$ non vide et on fixe $A \in \mathscr{C}_d(P)$ de coefficient dominant a_d.

4) Montrer que l'application $\left\{ \begin{array}{ccc} \mathscr{C}_1(P) & \longrightarrow & \mathbb{C}[X] \\ U & \longmapsto & U \circ A \end{array} \right.$ est à valeurs dans $\mathscr{C}_d(P)$ et injective.

5) Soit $B \in \mathscr{C}_d(P)$ de coefficient dominant b_d. On pose $c = \dfrac{b_d}{a_d}$.

a) Montrer que $c^n = c$.

b) Que dire du degré de $(B - cA) \circ P - \big(B^n - (cA)^n\big)$? En déduire que $B = cA$.

c) Calculer $P \circ (cA) - cP \circ A$ et en déduire que $cX \in \mathscr{C}_1(P)$.

d) Montrer finalement que $\big|\mathscr{C}_d(P)\big| = \big|\mathscr{C}_1(P)\big|$.

Pour tous $P, Q \in \mathbb{C}[X]$, on dit que $P \sim Q$ s'il existe un polynôme $U \in \mathscr{U}$ pour lequel $Q = U \circ P \circ U^{-1}$. On admet que $\sim$ est une relation d'équivalence sur $\mathbb{C}[X]$.

6) **a)** Montrer que tout polynôme non constant de $\mathbb{C}[X]$ est en relation par $\sim$ avec un polynôme unitaire et réduit.

b) Soient $P \in \mathbb{C}[X]$ de degré $n \geqslant 2$ et $d \in \mathbb{N}^*$. Montrer que si $\mathscr{C}_d(P)$ est non vide, alors $\big|\mathscr{C}_d(P)\big| = \big|\mathscr{C}_1(P)\big|$.

En résumé, pour tout $P \in \mathbb{C}[X]$ de degré au moins 2 et tout $d \in \mathbb{N}^*$, soit P ne commute à aucun polynôme de degré d, soit il y a autant de polynômes de degré d qui commutent à P que de polynôme de degré 1 qui le font.

3

1) Soit A un sous-anneau de $\mathbb{R}$. Montrer que l'ensemble $\mathscr{M}_2(A)$ des matrices carrées de taille 2 à coefficients dans A est un sous-anneau de $\mathscr{M}_2(\mathbb{R})$.

On admet que l'ensemble $\mathrm{U}\big(\mathscr{M}_2(A)\big)$ des inversibles de $\mathscr{M}_2(A)$, plutôt noté $\mathrm{GL}_2(A)$, est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

On s'intéresse dans ce problème à quelques propriétés des groupes $\mathrm{GL}_2(\mathbb{Q})$ et $\mathrm{GL}_2(\mathbb{Z})$.

On admet que pour tous $M,N \in \mathscr{M}_2(\mathbb{R})$: $\quad \det(MN) = \det(M)\det(N)$. La preuve de cette identité fondamentale ne présente pas de difficulté, il faut juste prendre le temps de l'écrire.

2) **a)** Montrer que $\mathrm{GL}_2(\mathbb{Z}) = \Big\{M \in \mathscr{M}_2(\mathbb{Z}) \mid \quad \det(M) = 1 \quad \text{ou} \quad \det(M) = -1\Big\}$.

b) Justifier que l'ensemble $\mathrm{SL}_2(\mathbb{Z}) = \Big\{M \in \mathrm{GL}_2(\mathbb{Z}) \mid \quad \det(M) = 1\Big\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$ sans utiliser la définition et la caractérisation des sous-groupes.

On pose $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Ces deux matrices appartiennent à $\mathrm{SL}_2(\mathbb{Z})$.

c) Calculer l'ordre des matrices S et T. En admettant que ST est d'ordre 6, en déduire que $\mathrm{SL}_2(\mathbb{Z})$ contient des éléments d'ordre 1, 2, 3, 4 et 6.

3) Soit $M \in \mathscr{M}_2(\mathbb{R})$. On pose $u_k = \mathrm{tr}\big(M^k\big)$ pour tout $k \in \mathbb{N}$.

a) Montrer que $M^2 - \mathrm{tr}(M)M + \det(M)I_2 = 0$, puis que la suite $(u_k)_{k\in\mathbb{N}}$ est récurrente linéaire d'ordre 2.

b) Montrer que si $\det(M) = -1$ et $\mathrm{tr}(M) > 0$, alors $|u_k| \xrightarrow[k\to+\infty]{} +\infty$.

c) En déduire que si M est d'ordre fini et appartient à $\mathrm{GL}_2(\mathbb{Z}) \smallsetminus \mathrm{SL}_2(\mathbb{Z})$, alors M est d'ordre 2. On pourra s'intéresser à $-M$.

4) Soit $M \in \mathrm{SL}_2(\mathbb{Z})$ d'ordre fini.

a) En adaptant la preuve de la question **3)b)**, montrer que $\mathrm{tr}(M) \leqslant 2$. En déduire que $\mathrm{tr}(M) \geqslant -2$.

b) Montrer que si $\mathrm{tr}(M) = -1$, alors $M^3 = I_2$, et que si $\mathrm{tr}(M) = 1$, alors $M^6 = I_2$.

c) On suppose que $\mathrm{tr}(M) = 2$. Calculer le reste de la division euclidienne de X^k par $(X-1)^2$ et en déduire que $M = I_2$.

d) Montrer que M est d'ordre 1, 2, 3, 4 ou 6.

On se tourne à présent vers $\mathrm{GL}_2(\mathbb{Q})$, mais un détour par les sous-groupes de $\mathbb{Z}^2$ s'impose en amont.

5) Soit H un sous-groupe non monogène de $\mathbb{Z}^2$. On note π l'application $(x,y) \longmapsto y$ de $\mathbb{Z}^2$ dans $\mathbb{Z}$.

a) Justifier l'existence d'un entier $n \in \mathbb{N}$ pour lequel $\pi(H) = n\mathbb{Z}$, puis montrer que $n \neq 0$.

On peut ainsi se donner un élément de H de la forme (m,n) avec $m \in \mathbb{Z}$.

b) Montrer que pour tout $h \in H$, il existe un et un seul couple $(q_h, r_h) \in \mathbb{Z}^2$ pour lequel $h = q_h(m,n) + (r_h, 0)$.

c) Montrer que l'application $h \longmapsto r_h$ est un morphisme de groupes de H dans $\mathbb{Z}$ et en déduire l'existence de deux éléments u et v de H pour lesquels $H = \mathbb{Z}u + \mathbb{Z}v$.

6) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$.

a) Justifier l'existence d'un entier $d \in \mathbb{N}^*$ pour lequel $dM \in \mathscr{M}_2(\mathbb{Z})$ pour tout $M \in G$.

On note H l'ensemble des sommes $\displaystyle\sum_{M\in G} dM \begin{pmatrix} x_M \\ y_M \end{pmatrix}$ dans lesquelles les x_M et les y_M sont des entiers quelconques qui dépendent de M.

b) Montrer que H est un sous-groupe de $\mathscr{M}_{2,1}(\mathbb{Z})$ contenant $\begin{pmatrix} d \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ d \end{pmatrix}$. Pourquoi H n'est-il pas monogène ? Montrer que pour tous $M \in G$ et $X \in H$: $\quad MX \in H$.

D'après **5)c)**, en identifiant toute colonne $\begin{pmatrix} x \\ y \end{pmatrix}$ au couple (x,y), il existe deux colonnes $X_1 \in H$ et $X_2 \in H$ pour lesquelles $H = \mathbb{Z}X_1 + \mathbb{Z}X_2$. On note P la matrice carrée de taille 2 de colonnes X_1 et X_2.

c) Justifier l'existence d'une matrice $Q \in \mathscr{M}_2(\mathbb{Z})$ pour laquelle $PQ = dI_2$, puis montrer que $P \in \mathrm{GL}_2(\mathbb{Q})$.

d) Montrer que $MP \in P\mathscr{M}_2(\mathbb{Z})$ pour tout $M \in G$, puis que $P^{-1}MP \in \mathrm{GL}_2(\mathbb{Z})$.

En résumé : $\quad P^{-1}GP \subset \mathrm{GL}_2(\mathbb{Z})$, $\quad$ donc G est conjugué à un sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$. À conjugaison près, les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$ sont ainsi les mêmes que ceux de $\mathrm{GL}_2(\mathbb{Z})$. Alors certes, on n'a pas pas déterminé explicitement les sous-groupes de $\mathrm{GL}_2(\mathbb{Z})$ dans ce problème, mais on n'en est pas loin !