Devoir surveillé

1 On pose : $A = \begin{pmatrix} 3 & 1 & -3 \\ 2 & 4 & -6 \\ 1 & 1 & -1 \end{pmatrix}$.

1) Montrer que A^2 est combinaison linéaire de I_3 et A.

2) En déduire que A est inversible et calculer son inverse.

3) En déduire également une expression explicite coefficient par coefficient de A^n pour tout $n \in \mathbb{N}$.

---

2 On rappelle que : $\mathrm{j} = \mathrm{e}^{\frac{2i\pi}{3}}$. Pour tous $x, y, z \in \mathbb{C}$, on note $C(x,y,z)$ la matrice $\begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}$, dite *circulante* (de taille 3). On note $\mathscr{C}$ l'ensemble de ces matrices : $\mathscr{C} = \Big\{ C(x,y,z) \mid \ x,y,z \in \mathbb{C} \Big\}$ et on pose : $U = C(0,1,0)$.

1) Structure de $\mathscr{C}$:

a) Montrer que $\mathscr{C}$ est l'ensemble des matrices de $\mathscr{M}_3(\mathbb{C})$ qui commutent à U.

b) En déduire que $\mathscr{C}$ est un sous-anneau et un sous-espace vectoriel de $\mathscr{M}_3(\mathbb{C})$.

c) Calculer U^k pour tout $k \in \mathbb{N}$.

d) Montrer que : $\mathscr{C} = \mathbb{C}[U]$ où $\mathbb{C}[U]$ est l'ensemble des *polynômes en* U, i.e. des matrices de la forme $P(U)$ avec $P \in \mathbb{C}[X]$. Qu'en déduit-on sur l'anneau $\mathscr{C}$?

2) Diagonalisation des éléments de $\mathscr{C}$: On note à présent J la matrice $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \mathrm{j} & \mathrm{j}^2 \\ 1 & \mathrm{j}^2 & \mathrm{j} \end{pmatrix}$ et $\overline{J}$ sa matrice conjuguée coefficient par coefficient.

a) Simplifier $J\overline{J}$ et $\overline{J}J$. Qu'en déduit-on ?

b) Montrer que pour toute matrice diagonale $D \in \mathscr{M}_3(\mathbb{C})$: $JDJ^{-1} \in \mathscr{C}$.

c) Montrer que pour tout $M \in \mathscr{C}$, il existe une matrice diagonale $D(M) = \mathrm{diag}\Big(d_1(M), d_2(M), d_3(M)\Big) \in \mathscr{M}_3(\mathbb{C})$ pour laquelle : $MJ = JD(M)$.

3) Inversibles de l'anneau $\mathscr{C}$: Montrer que : $\mathrm{U}(\mathscr{C}) = \Big\{ M \in \mathscr{C} \mid \ \forall k \in [\![1,3]\!], \ \ d_k(M) \neq 0 \Big\}$.

---

3 On fixe un entier naturel non nul n. On note :

— $\mathbb{Z}[X]$ l'ensemble des polynômes à une indéterminée X à coefficients dans $\mathbb{Z}$,

— $\mathscr{K}_n$ l'ensemble des polynômes de $\mathbb{Z}[X]$ unitaires de degré n dont les racines dans $\mathbb{C}$ sont toutes non nulles et de module inférieur ou égal à 1,

— $\mathscr{R}_n$ l'ensemble des racines des polynômes éléments de $\mathscr{K}_n$.

1) a) Montrer que pour tout $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathscr{K}_n$: $|a_0| = 1$ et $|a_{n-1}| \leqslant n$.

b) Montrer que : $\mathscr{R}_n \subset \mathbb{U}$.

2) Soit $P = (X-\alpha)(X-\beta) \in \mathscr{K}_2$ avec $\alpha, \beta \in \mathbb{C}$.

a) Montrer que si α n'est pas un réel : $P \in \Big\{ X^2 - X + 1 \ , \ X^2 + 1 \ , \ X^2 + X + 1 \Big\}$.

b) Que peut valoir P si α est un réel ?

c) Montrer que : $\mathscr{R}_2 \subset \mathbb{U}_{12}$.

3) Soit $P \in \mathbb{Z}[X]$ de degré n.

a) Montrer qu'il existe un et un seul polynôme $\widehat{P} \in \mathbb{Z}[X]$ de degré n pour lequel : $P(X)P(-X) = (-1)^n \widehat{P}\big(X^2\big)$.

b) Décrire la forme scindée sur $\mathbb{C}$ de $\widehat{P}$ en fonction de celle de P.

c) Montrer que si : $P \in \mathscr{K}_n$, alors : $\widehat{P} \in \mathscr{K}_n$.

d) En déduire que l'ensemble $\mathscr{R}_n$ est stable par la fonction $z \longmapsto z^2$.

4) a) Montrer que l'ensemble $\Big\{\big|\sigma_k(P)\big| \ \big| \quad k \in [\![1,n]\!] \quad \text{et} \quad P \in \mathscr{K}_n\Big\}$ est majoré, où $\sigma_1(P),\ldots,\sigma_n(P)$ désignent évidemment les fonctions symétriques élémentaires de P.

b) Soit $N \in \mathbb{N}$. Combien existe-t-il de polynômes $P \in \mathbb{Z}[X]$ unitaires de degré n à coefficients dans $[\![-N,N]\!]$?

c) En déduire que l'ensemble $\mathscr{R}_n$ est fini.

5) a) Montrer, en exploitant les résultats précédents, que tout élément de $\mathscr{R}_n$ appartient à $\mathbb{U}_r$ pour un certain $r \in \mathbb{N}^*$.

b) En déduire que : $\quad \mathscr{R}_n \subset \mathbb{U}_r \quad$ pour un certain $r \in \mathbb{N}^*$ (*théorème de Kronecker*).

c) En déduire que pour tout $P \in \mathscr{K}_n$, il existe un entier $s \in \mathbb{N}^*$ pour lequel P divise $\big(X^r - 1\big)^s$.

---

4 Vous ne vous lancez dans cet exercice que si vous avez réussi parfaitement ou presque tout le reste du devoir.

Soit G un groupe. On dit qu'un élément x de G est *d'ordre fini* si pour un certain $n \in \mathbb{N}^*$: $\quad x^n = 1_G$. $\quad$ On note F l'ensemble des éléments d'ordre fini de G et, pour tout $k \in \mathbb{N}^*$, F_k l'ensemble des produits de k éléments de F.

1) Montrer que pour tous $x \in F$, $k \in \mathbb{Z}$ et $g \in G$: $\quad x^k \in F \quad$ et $\quad g^{-1}xg \in F$.

2) Montrer — sans utiliser aucun théorème de Lagrange ! — que tout sous-groupe fini de G est inclus dans F.

3) Montrer que pour tous $k \in \mathbb{N}^*$ et $x_1,\ldots,x_k \in F$: $\quad x_1x_2\ldots x_{k-1}x_kx_1 \in F_k$.

On suppose à présent que F est fini et on note N son cardinal.

4) Montrer que pour tout $k \geqslant N$: $\quad F_k \subset F_N$.

5) Montrer que F_N est un sous-groupe de G.

6) Montrer enfin que F est un sous-groupe de G.
