# Contrôle final

*Calculatrice et documents sont interdits.*
*Tous les résultats doivent être correctement rédigés et rigoureusement justifiés.*
*Durée de l'épreuve : 2h.*
*Le barême est donné à titre indicatif.*

## Exercice 1 : triangularisation de matrice. *(5 points)*

Soit $M = \begin{pmatrix} 4 & 3 & -6 \\ -1 & 2 & 0 \\ 1 & 2 & -2 \end{pmatrix}$ dans $\mathcal{M}_3(\mathbf{R})$. Le but de cet exercice est de déterminer les puissances de $M$. Pour cela, nous utiliserons une triangularisation de $M$.

Soient $a$ et $b$ des nombres réels. Notons $T = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix}$. Posons également $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 2 \\ 1 & 1 & 1 \end{pmatrix}$.

1. Calculer $T^2$, $T^3$ et $T^4$. Déterminer l'expression de $T^n$ pour tout $n \in \mathbf{N}$.
2. Montrer que $P$ est inversible et calculer son inverse.
3. Calculer $P^{-1}MP$.
4. En déduire l'expression de $M^n$ pour tout $n \in \mathbf{N}$.

## Exercice 2 : groupe de Galois.

Soit $n \in \mathbf{N}^*$ et $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré $n$ à coefficients rationnels : $\forall\, k \leq n,\ a_k \in \mathbf{Q}$.

Soit $K$ un certain sous-corps de $(\mathbf{C}, +, \times)$ contenant $\mathbf{Q}$ et toutes les racines complexes de $P$.[1] La connaissance précise de $K$ n'a aucune importance pour cet exercice.

Soit $G$ l'ensemble des isomorphismes du corps $(K, +, \times)$ qui préservent $\mathbf{Q}$. Il s'agit de l'ensemble des bijections $f$ de $K$ vers $K$ telles que :
- $\forall (x, y) \in K^2,\quad f(x + y) = f(x) + f(y)$,
- $\forall (x, y) \in K^2,\quad f(xy) = f(x)f(y)$,
- $\forall r \in \mathbf{Q},\quad f(r) = r$.

1. Étude théorique. *(5 points)*
   (a) Montrer que l'application $f$ définie de $K$ vers $K$ par $f(z) = \bar{z}$ est dans le groupe $G$.
   (b) Montrer que $G$ est un sous-groupe du groupe $(Bij(K), \circ)$.
   (c) Soit $z \in \mathbf{C}$ une racine de $P$ et soit $f \in G$.
   Calculer $f(P(z))$ et montrer que $f(z)$ est aussi une racine de $P$.
   (d) En déduire que tout élément de $G$ réalise une permutation des racines du polynôme $P$.

1. Il s'agit du corps appelé corps de décomposition de $P$. C'est le plus petit sous-corps de $\mathbf{C}$ contenant $\mathbf{Q}$ et les racines de $P$.

Reformulons ce dernier résultat. Notons $z_1, z_2, \ldots, z_n$ les $n$ racines de $P$. À tout élément $f$ de $G$, on peut donc associer la permutation $\sigma_f$ de $\mathfrak{S}_n$ définie par $\sigma_f(i) = j$ si $f(z_i) = z_j$.
Par exemple, si $P$ a trois racines $z_1, z_2$ et $z_3$ et si $f(z_1) = z_3$, $f(z_2) = z_2$ et $f(z_3) = z_1$, alors $\sigma_f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$.

Comme $\sigma_f$ représente simplement la restriction de la bijection $f$ aux racines de $P$, l'application $f \mapsto \sigma_f$ est naturellement un morphisme de groupe entre $(G, \circ)$ et $(\mathfrak{S}_n, \circ)$. L'ensemble $\{\sigma_f \in \mathfrak{S}_n ; f \in G\}$ est l'image de ce morphisme et est donc un sous-groupe de $(\mathfrak{S}_n, \circ)$.

Ce sous-groupe des permutations réalisées par les éléments de $G$ est appelé groupe de Galois associé à $P$. Dans la théorie de Galois, c'est l'étude de ce sous-groupe de $\mathfrak{S}_n$ qui permet d'obtenir des résultats sur les racines de $P$.

2. Premier exemple : soit $P = X^3 - 1$. *(3,5 points)*

   (a) Déterminer les racines de $P$ et les numéroter.

   (b) Comment l'application $f : z \mapsto \bar{z}$ permute-t-elle les racines de $P$ ?

   (c) Les racines de $P$ peuvent-elles être permutées autrement par des éléments de $G$ ? Donner le groupe de Galois associé à $P$.

3. Second exemple : soit $P = X^3 - 3X + 1$. *(8 points)*

   Nous allons déterminer le groupe de Galois de $P$ sans calculer explicitement ses racines.

   (a) Montrer que $P$ n'a pas de racine dans $\mathbf{Q}$.
   *On pourra utiliser la propriété suivante : si une fraction irréductible $\frac{p}{q} \in \mathbf{Q}$ est racine d'un polynôme $P = \sum_{k=0}^{n} a_k X^k$ à coefficients entiers, alors l'entier $p$ divise $a_0$ et l'entier $q$ divise son coefficient dominant $a_n$.*

   (b) En déduire que $P$ est irréductible dans $\mathbf{Q}[X]$.
   Soit $\alpha \in \mathbf{C}$ une racine de $P$.

   (c) Montrer que $\alpha^3 = 3\alpha - 1$. En déduire des expressions de $\alpha^4$ et de $\alpha^6$ en fonction de $\alpha$ et $\alpha^2$.

   (d) Montrer que $\beta = \alpha^2 - 2$ est aussi racine de $P$.

   (e) Montrer que $P$ et $X^2 - X - 2$ sont premiers entre eux et en déduire $\alpha \neq \beta$.

   (f) Montrer alors que $\gamma = -\alpha - \beta$ est la troisième racine de $P$.
   *On admet qu'on peut montrer comme ci-dessus que $\gamma$ est distinct de $\alpha$ et $\beta$.*

   (g) Soit $f_1$ un élément de $G$ tel que $f_1(\alpha) = \beta = \alpha^2 - 2$. Montrer que nécessairement $f_1(\beta) = \gamma$ puis en déduire $f_1(\gamma)$.

   (h) De même, soit $f_2$ un élément de $G$ tel que $f_2(\alpha) = \gamma$. Calculer alors $f_2(\beta)$ puis en déduire $f_2(\gamma)$.
   *On admet pour la suite l'existence de ces isomorphismes $f_1$ et $f_2$.*

   (i) Supposons qu'il existe un élément $g$ de $G$ tel que $g(\alpha) = \alpha$, $g(\beta) = \gamma$ et $g(\gamma) = \beta$. Étudier alors $g \circ f_1$ et aboutir à une contradiction avec le résultat de la question (h).

   (j) Donner le groupe de Galois associé à $P$.