Contrôle 4

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 $n \in \mathbf{N}$.

   Montrons par récurrence que pour tout entier $n \in \mathbf{N}$, $T^n = \begin{pmatrix} 1 & an & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b^n \end{pmatrix}$.
   Le résultat est vrai pour $n = 0$ (avec $T^0 = I_3$) et $n = 1$.
   Supposons maintenant le résultat vrai pour un certain entier n. Alors

   $$T^{n+1} = TT^n = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} 1 & an & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b^n \end{pmatrix} = \begin{pmatrix} 1 & an+a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b^{n+1} \end{pmatrix}.$$

   Le résultat est donc encore valable au rang $n+1$ et la preuve est terminée.
2. Montrer que P est inversible et calculer son inverse.

   On effectue l'algorithme de Gauss. Celui-ci permet de montrer que P est inversible et on obtient $P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -2 \\ -2 & -1 & 3 \end{pmatrix}$.
3. Calculer $P^{-1}MP$.

   On obtient $P^{-1}MP = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. C'est la matrice T avec $a = 3$ et $b = 2$.
4. En déduire l'expression de M^n pour tout $n \in \mathbf{N}$.

   Comme $P^{-1}MP = T$, $M = PTP^{-1}$. Donc pour tout entier n, $M^n = (PTP^{-1})^n = PT^nP^{-1}$. D'après la question 1, on obtient

   $$M^n = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 2 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2^n \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -2 \\ -2 & -1 & 3 \end{pmatrix}.$$

Et finalement

$$M^n = \begin{pmatrix} 3n+1 & 3n & -6n \\ 3n+4-4\times 2^n & 3n+3-2\times 2^n & -6n-6+6\times 2^n \\ 3n+2-2\times 2^n & 3n+1-2^n & -6n-2+3\times 2^n \end{pmatrix}.$$

Notons que cette expression est bien valable pour $n = 0$.

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.

   Il y a quatre propriétés à vérifier.
   Tout d'abord, on sait que la conjugaison complexe f est une bijection dont la bijection réciproque est f elle-même. Donc si on admet que f est bien définie sur K, alors elle est bijective de K vers K.
   Soient x et y dans K. Alors $f(x+y) = \overline{x+y} = \bar{x} + \bar{y} = f(x) + f(y)$.
   De même, $f(xy) = \overline{xy} = \bar{x}\bar{y} = f(x)f(y)$.
   Enfin, tout nombre réel est égal à son conjugué. En particulier, $\forall r \in \mathbf{Q}, f(r) = \bar{r} = r$.

   Ainsi, f est bien un élément de G.

   (b) Montrer que G est un sous-groupe du groupe $(Bij(K), \circ)$.

   Montrons les trois propriétés que doit satisfaire un sous-groupe.
   Soient f et g dans G. Alors $f \circ g$ est une bijection de K. Soient x et y dans G. Alors $f \circ g(x+y) = f(g(x) + g(y)) = f(g(x)) + f(g(y)) = f \circ g(x) + f \circ g(y)$. De même, $f \circ g(xy) = f \circ g(x) f \circ g(y)$. Enfin, pour tout rationnel r, $f \circ g(r) = f(g(r)) = f(r) = r$. Donc $f \circ g \in G$.
   L'application Id sur K est clairement un élément de G.
   Soit $f \in G$. Montrons que $f^{-1} \in G$. Soient x et y dans K. Comme f est uen bijection, il existe a et b dans K tels que $f(a) = x$ et $f(b) = y$. Alors $f^{-1}(x+y) = f^{-1}(f(a) + f(b)) = f^{-1}(f(a+b)) = a+b = f^{-1}(x) + f^{-1}(b)$. De même $f^{-1}(xy) = f^{-1}(x) f^{-1}(y)$.
   Enfin, soit $r \in \mathbf{Q}$, alors $f(r) = r$. Donc $f^{-1}(r) = r$. Ains $f^{-1} \in G$.
   On peut conclure que G est bien un sous-groupe de $Bij(K)$.

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.

(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.

Calculons en utilisant les propriétés de f : $f(P(z)) = f(\sum_{k=0}^{n} a_k z^k) = \sum_{k=0}^{n} f(a_k z^k)$ (f est un morphisme additif). Donc $f(P(z)) = \sum_{k=0}^{n} f(a_k)(f(z))^k$ (f est aussi un morphisme multiplicatif). De plus, les a_k sont des rationnels, donc $f(P(z)) = \sum_{k=0}^{n} a_k (f(z))^k$ (f préserve les rationnels). Enfin, comme z est racine de P, $P(z) = 0$. Donc $f(P(z)) = f(0) = 0$. On obtient finalement $\sum_{k=0}^{n} a_k (f(z))^k = 0$, donc $P(f(z)) = 0$. Ainsi, si z est racine de P, $f(z)$ est aussi racine de P.

(d) En déduire que tout élément de G réalise une permutation des racines du polynôme P.

Soit $f \in G$. On a montré que l'image par f d'une racine de P est une racine de P. Donc si on note S l'ensemble des racines de P, alors $f(S) \subset S$. Or on sait de plus que f est une bijection. Donc comme S est fini (de cardinal au plus n), f réalise une bijection de S vers S. Autrement dit, f réalise une permutation des 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 σ_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 σ_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.
Les racines de P sont les raciens cubiques de 1. Il s'agit des nombres $z_1 = 1$, $z_2 = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$ et $z_3 = e^{-\frac{2i\pi}{3}} = \frac{-1-i\sqrt{3}}{2}$.

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

Notons f l'application $z \mapsto \bar{z}$. On a $f(1) = 1$, $f(e^{\frac{2i\pi}{3}}) = e^{-\frac{2i\pi}{3}}$ et $f(e^{-\frac{2i\pi}{3}}) = e^{\frac{2i\pi}{3}}$. Donc $f(z_1) = z_1$, $f(z_2) = z_3$ et $f(z_3) = z_2$. La bijection f échange z_2 et z_3. Sa permutation associée est $\sigma_f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in \mathfrak{S}_3$. C'est la transposition τ_{23}.

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

Tout élément de G préserve les rationnels. En particulier $\forall g \in G$, $g(1) = 1$. Donc z_1 est toujours envoyé sur lui-même. Ainsi un élément de G ne peut que fixer les trois racines ou échanger z_2 et z_3. Il n'y a donc que deux permutations possibles et le groupe de Galois associé à P est $\{Id, \tau_{23}\}$.

3. Second exemple : soit $P = X^3 - 3X + 1$. *(7 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.

Supposons que P a une racine rationnelle écrite sous forme irréductible $\frac{p}{q}$. Alors, d'après la propriété, on aurait $p|1$ et $q|1$. Donc $p = \pm 1$, $q = \pm 1$ et $\frac{p}{q} = \pm 1$. Ainsi, les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1 \neq 0$ et $P(-1) = 3 \neq 0$. On en déduit que P n'a aucune racine dans $\mathbf{Q}$.

(b) En déduire que P est irréductible dans $\mathbf{Q}[X]$.
D'après le cours, un polynôme de degré 3 sans racine est irréductible. Comme c'est le cas de P dans $\mathbf{Q}[X]$, on en déduit qu'il est irréductible dans $\mathbf{Q}[X]$.
Rappelons l'argument : si P était réductible dans $\mathbf{Q}[X]$, on pourrait l'écrire comme un produit de deux polynômes non constants de $\mathbf{Q}[X]$. Comem P est de degré 3, ce serait nécessairement le produit d'un polynôme de degré 1 et d'un polynôme de degré 2. Or l'existence de ce facteur de degré 1 signifie que P possède une racine dans $\mathbf{Q}$ ce qui est faux.

Soit $\alpha \in \mathbf{C}$ une racine de P.

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

Comme α est racine de P, $P(\alpha) = 0$. Donc $\alpha^3 - 3\alpha + 1 = 0$. Donc $\alpha^3 = 3\alpha - 1$.
On en déduit $\alpha^4 = \alpha\alpha^3 = 3\alpha^2 - \alpha$ et $\alpha^6 = (\alpha^3)^2 = (3\alpha - 1)^2 = 9\alpha^2 - 6\alpha + 1$.

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

Calculons $P(\beta)$:

$$\begin{aligned} P(\beta) &= \beta^3 - 3\beta + 1 \\ &= (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 \\ &= (\alpha^6 - 6\alpha^4 + 12\alpha^2 - 8) - 3\alpha^2 + 7 \\ &= (9\alpha^2 - 6\alpha + 1) - 6(3\alpha^2 - \alpha) + 9\alpha^2 - 1 \\ &= 0. \end{aligned}$$

Donc β est bien racine de P.

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

Nous proposons trois méthodes pour montrer que P et $Q = X^2 - X - 2$ sont premiers entre eux.
On peut calculer le PGCD de P et Q en utilisant l'algorithme d'Euclide qui est ici très rapide. Division euclidienne de P par Q : $P = (X + 1)Q + 3$. Comme le reste est un polynôme constant non nul, on en déduit que $PGCD(P, Q) = 1$ et donc que P et Q sont premiers entre eux.
On peut ici factoriser Q : $Q = (X + 1)(X - 2)$. Les facteurs irréductibles de Q sont donc $X + 1$ et $X - 2$. Or -1 et 2 ne sont pas racines de P (car ce sont des rationnels), donc P n'a pas de facteur commun avec Q. Donc P et Q sont premiers entre eux.
Dernier argument possible : le calcul du PGCD ne dépend pas du corps dans lequel on se place. Ainsi, le PGCD de P et Q sera le même dans $\mathbf{Q}[X]$, $\mathbf{R}[X]$ et $\mathbf{C}[X]$. Comme P est irréductible dans $\mathbf{Q}[X]$, il ne peut avoir de facteur commun avec Q

autre que 1 ou lui-même. Comme P ne divise pas Q, on en déduit que P et Q sont premiers entre eux.

(f) En déduire que $\gamma = -\alpha - \beta$ est également racine de P.

D'après les questions précédentes, on connaît deux racines de P. Reste à déterminer la troisième. Or on sait que la somme des racines d'un polynôme de degré n est égale à l'opposé du coefficient a_{n-1}. Ici, le coefficient a_2 est nul. Donc la somme des racines de P est nulle. On en déduit que $\gamma = -\alpha - \beta$ est la troisième racine de P.

On admet qu'on peut montrer comme ci-dessus que γ est distinct de α et β.

(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 $f_1(\gamma)$.

On rappelle que f_1 est un isomorphisme de corps. Donc $f_1(\beta) = f_1(\alpha^2 - 2) = (f_1(\alpha))^2 - f_1(2)$. Or $f_1(\alpha) = \beta = \alpha^2 - 2$ et comme $2 \in \mathbf{Q}$, donc $f_1(2) = 2$. Donc $f_1(\beta) = (\alpha^2 - 2)^2 - 2 = \alpha^4 - 4\alpha^2 + 4 - 2 = (3\alpha^2 - \alpha) - 4\alpha^2 + 2 = -\alpha - (\alpha^2 - 2)$. Donc $f_1(\beta) = \gamma$. On sait de plus que f_1 permute les racines, donc $f_1(\gamma) = \alpha$.

(h) De même, soit f_2 un élément de G tel que $f_2(\alpha) = \gamma$. Calculer alors $f_2(\beta)$ puis en déduire $f_2(\gamma)$.

Le calcul est le même : $f_2(\beta) = (f_2(\alpha))^2 - 2 = (-\alpha - \beta)^2 - 2 = \alpha$. Et donc $f_2(\gamma) = \beta$.

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).

Regardons l'image des racines de P par $g \circ f_1$: $g \circ f_1(\alpha) = g(\beta) = \gamma$, $g \circ f_1(\beta) = g(\gamma) = \beta$ et donc $g \circ f_1(\gamma) = \alpha$. Comme f_1 et g sont dans le groupe $(G, \circ)$, $g \circ f_1 \in G$. Or on a vu à la question (h) que si un élément de G envoie α sur γ, alors nécessairement, il envoie β sur α. Ce n'est pas le cas de $g \circ f_1$ et on aboutit donc à une contradiction. On en déduit qu'un tel élément g n'existe pas.

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

Regardons les différentes permutations possibles des racines. Numérotons les racines : $z_1 = \alpha$, $z_2 = \beta$ et $z_3 = \gamma$. Soit $f \in G$. Si $f(\alpha) = \beta$, alors on a vu dans (g) que nécessairement $f(\beta) = \gamma$ et $f(\gamma) = \alpha$. alors f correspond à la permutation $\sigma_f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_3$.
Si $f(\alpha) = \gamma$, alors on a vu dans (h) que nécessairement $f(\beta) = \alpha$ et $f(\gamma) = \beta$. alors f correspond à la permutation $\sigma_f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.
Enfin, si $f(\alpha) = \alpha$, alors on a vu dans (i) que f ne pouvait pas échanger β et γ. Donc f fixe les trois racines et f correspond ainsi à la permutation $\sigma_f = Id$.
On a étudié tous les cas possibles et on sait (admis) que ces trois cas sont réalisés par certains éléments de G. On en déduit que le groupe de Galois associé à P est $\{Id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$.