Contrôle final

Calculatrice et documents sont interdits.
Tous les résultats doivent être correctement rédigés et rigoureusement justifiés.
Le barème est donné à titre indicatif.
La qualité de la rédaction sera fortement prise en compte dans la notation.

Exercice 1 : décomposition d'une permutation en 3-cycles (8 pts)

Soit $n \in \mathbf{N}^*$ et $(\mathfrak{S}_n, \circ)$ le groupe des permutations correspondant. On rappelle que pour deux permutations σ_1 et σ_2 dans $\mathfrak{S}_n$, $\sigma_1\sigma_2$ désigne la composée $\sigma_1 \circ \sigma_2$. On rappelle également que pour i et j deux éléments distincts de $[\![1, n]\!]$, τ_{ij} désigne la transposition qui échange i et j.

Pour i, j et k des éléments **distincts** de $[\![1, n]\!]$, on note $(i\ j\ k)$ le 3-cycle de $\mathfrak{S}_n$ qui permute i, j et k dans cet ordre. Il s'agit de la permutation qui envoie i sur j, j sur k et k sur i et qui fixe tous les autres éléments de $[\![1, n]\!]$ (schématisée par $i \mapsto j \mapsto k \mapsto i$).

On admet enfin le résultat suivant :
Théorème : toute permutation de $\mathfrak{S}_n$ peut s'écrire comme une composée de transpositions. Une telle écriture n'est pas unique mais il y a tout de même une propriété invariante : si une permutation σ peut s'écrire comme une composée de r transpositions mais également comme une composée de s autres transpositions, alors r et s ont la même parité.

Le but de cet exercice est de caractériser les permutations que l'on peut écrire comme une composée de 3-cycles.

1. Soient i, j et k des éléments distincts. Calculer la composée $\tau_{ij}\tau_{jk}$ et reconnaître un 3-cycle.

   On compose τ_{ij} et τ_{jk} et on obtient la permutation qui envoie i sur j, j sur k et k sur i. Il s'agit du cycle $(i\ j\ k)$.

2. Soient i, j, k et ℓ des entiers distincts de $[\![1, n]\!]$. Calculer la composée $(i\ j\ k)(k\ \ell\ j)$ et reconnaître une composée de deux transpositions.

   On compose $(i\ j\ k)$ et $(k\ \ell\ j)$ et on obtient la permutation qui envoie i sur j, j sur i, k sur ℓ et ℓ sur k. Elle échange donc i et j, ainsi que k et ℓ. Donc $(i\ j\ k)(k\ \ell\ j) = \tau_{ij}\tau_{k\ell} = \tau_{k\ell}\tau_{ij}$.

3. Soit $\sigma \in \mathfrak{S}_n$ une permutation que l'on peut décomposer en un produit d'un nombre pair de transpositions. Montrer, à l'aide des deux questions précédentes, que σ peut se décomposer en un produit de 3-cycles.

   Par hypothèse, σ eut s'écrire comme un produit d'un nombre pair p de transpositions. Numérotons-les $\tau_1, \tau_2, \ldots, \tau_p$: $\sigma = \tau_1\tau_2 \cdots \tau_{p-1}\tau_p$.
   D'après les questions 1 et 2, un produit de deux transpositions est soit égal à un 3-cycle (si les transpositions ont un terme en commun), soit égal à un produit de deux 3-cycles (si les transpositions sont disjointes). Ainsi, dans l'écriture de σ, on peut remplacer $\tau_1\tau_2$

par un 3-cycle ou un produit de 3-cycles. De même pour $\tau_3\tau_4$, $\tau_5\tau_6$ et ainsi de suite jusqu'à $\tau_{p-1}\tau_p$ puisque p est pair.

Conclusion : en remplaçant, dans la décomposition de σ chaque paire de transpositions successives par un ou deux 3-cycles, on obtient finalement une décomposition de σ en un produit de 3-cycles.

4. Soit $\sigma \in \mathfrak{S}_n$ une permutation que l'on peut décomposer en un produit d'un nombre impair de transpositions. Montrer, à l'aide de la question 1 et du résultat admis en introduction, que σ ne peut pas se décomposer en un produit de 3-cycles.

   On considère maintenant que σ se décompose en un produit d'un nombre impair de transpositions. Supposons par l'absurde que σ puisse se décomposer en un produit de 3-cycles. Notons-les $c_1, c_2, \ldots, c_q$: $\sigma = c_1c_2\cdots c_q$. D'après la question 1, tout 3-cycle peut s'écrire comme un produit de deux transpositions. En remplaçant chacun des q 3-cycles c_i par un tel produit, on obtient une décomposition de σ en un produit de $2q$ transpositions.

   Or σ se décompose par hypothèse en un produit d'un nombre impair de transpositions. On obtient une contradiction avec le théorème énoncé en début d'exercice.

   Donc σ ne peut pas se décomposer en un produit de 3-cycles.

   Conclusion : une permutation est décomposable en un produit de 3-cycles si et seulement si σ se décompose en un nombre pair de transpositions.

5. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} \in \mathfrak{S}_5$. Déterminer, si cela est possible, une décomposition de σ en 3-cycles.

   La question 3 nous suggère une méthode : on peut commencer par décomposer σ en un produit de transpositions, puis remplacer chaque paire de transposition par un 3-cycle.

   Appliquons l'algorithme étudié en cours : on obtient $\sigma = \tau_{25}\tau_{34}\tau_{23}\tau_{12}$. D'après la question 2, $\tau_{23}\tau_{12} = (1\ 3\ 2)$ et d'après la question 3, $\tau_{25}\tau_{34} = (3\ 4\ 2)(2\ 5\ 4)$. Donc $\sigma = (3\ 4\ 2)(2\ 5\ 4)(1\ 3\ 2)$.

   On peut également essayer de trouver une décomposition directement en s'inspirant de l'algorithme du cours. On souhaite ranger les éléments de la permutation σ dans l'ordre en la composant avec des 3-cycles. Pour remettre 5 à sa place il faudra que 2 soit envoyé sur 5. Et en envoyant 5 sur 3, on remettra aussi 3 à sa place. On calcule $(2\ 5\ 3)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$. On continue en envoyant 2 sur 4 et 4 sur 1 : $(2\ 4\ 1)(2\ 5\ 3)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id$. On en déduit $\sigma = (2\ 5\ 3)^{-1}(2\ 4\ 1)^{-1} = (2\ 3\ 5)(2\ 1\ 4)$.

6. Les permutations pouvant se décomposer en 3-cycles forment un sous-groupe de $\mathfrak{S}_n$. Combien y en a-t-il dans $\mathfrak{S}_4$? Les donner toutes.
   On pourra utiliser le théorème de Lagrange.

   Il y a 8 3-cycles dans $\mathfrak{S}_4$: $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$. Ces 8 permutations s'écrivent trivialement comme produit de un 3-cycle. Dans notre sous-groupe, il y a également l'identité id qui s'écrit comme un produit de 0 3-cycle.

   D'après le théorème de Lagrange, le sous-groupe que nous cherchons a un cardinal qui divise 24, le cardinal de $\mathfrak{S}_4$. Comme il contient au moins 9 éléments, il est de cardinal 12

ou 24. Or les transpositions se décomposant en un nombre impair (1) de transpositions, elles n'appartiennent pas au sous-groupe. Ce sous-groupe est donc de cardinal 12.
En plus des 8 3-cycles et de l'identité id, il y a les 3 double transpositions $\tau_{12}\tau_{34}, \tau_{13}\tau_{24}, \tau_{14}\tau_{23}$ d'après la question 2. Ainsi, le groupe des permutations se décomposant en 3-cycles est

$$\{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \tau_{12}\tau_{34}, \tau_{13}\tau_{24}, \tau_{14}\tau_{23}\}.$$

Exercice 2 : matrices et nombres complexes (15 pts)

Dans $\mathcal{M}_2(\mathbf{R})$, l'ensemble des matrices réelles de taille 2, on note 0_2 la matrice nulle, I_2 la matrice identité et $\mathrm{GL}_2(\mathbf{R})$ l'ensemble des matrices inversibles.
Pour $(x, y) \in \mathbf{R}^2$, on note $M_{x,y} = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$.
On note G l'ensemble des matrices de cette forme : $G = \{M_{x,y}\ ;\ (x, y) \in \mathbf{R}^2\}$.
On note enfin $G^* = G \setminus \{0_2\}$.

1. **Structure de groupe**

   (a) Soient x, y, x' et y' des nombres réels. Calculer le produit $M_{x,y}M_{x',y'}$.

   On calcule $M_{x,y}M_{x',y'} = \begin{bmatrix} xx' - yy' & -xy' - yx' \\ yx' + xy' & -yy' + xx' \end{bmatrix} = M_{xx'-yy',xy'+x'y}$.

   (b) Soit $(x, y) \neq (0, 0)$. Montrer que $M_{x,y}$ est une matrice inversible et donner l'expression de son inverse.

   On souhaite appliquer l'algorithme de Gauss. Il faut pour cela distinguer deux cas, sans quoi certaines opérations élémentaires sont impossibles.
   Soit $(x, y) \in \mathbf{R}^2 \setminus \{(0, 0)\}$.
   Si $x \neq 0$, on effectue dans cet ordre les opérations $L_2 \leftarrow L_2 - \frac{y}{x}L_1$, $L_1 \leftarrow L_1 + \frac{xy}{x^2+y^2}L_2$, $L_1 \leftarrow \frac{1}{x}L_1$, $L_2 \leftarrow \frac{x}{x^2+y^2}L_2$. On conclut que $M_{x,y}$ est inversible et son inverse est

   $$M_{x,y} = \begin{bmatrix} \frac{x}{x^2+y^2} & \frac{y}{x^2+y^2} \\ -\frac{y}{x^2+y^2} & \frac{x}{x^2+y^2} \end{bmatrix}.$$

   Si $x = 0$, alors $y \neq 0$ car $(x, y) \neq (0, 0)$. on effectue les opérations $L_1 \leftrightarrow L_2$ puis $L_1 \leftarrow \frac{1}{y}L_1$ et $L_2 \leftarrow -\frac{1}{y}L_2$. On obtient encore que $M_{x,y}$ est inversible et $M_{x,y}^{-1} = \begin{bmatrix} 0 & \frac{1}{y} \\ -\frac{1}{y} & 0 \end{bmatrix}$.
   Dans les deux cas, la matrice est inversible et son inverse est donnée par

   $$M_{x,y} = \begin{bmatrix} \frac{x}{x^2+y^2} & \frac{y}{x^2+y^2} \\ -\frac{y}{x^2+y^2} & \frac{x}{x^2+y^2} \end{bmatrix}.$$

   (c) Montrer que G^* est un sous-groupe de $(\mathrm{GL}_2(\mathbf{R}), \times)$.

   • Soient $M_{x,y}$ et $M_{x',y'}$ dans G^*. Alors d'après la question a., leur produit est égal à $M_{x,y}M_{x',y'} = M_{xx'-yy',xy'+x'y}$. En particulier c'est un élément de G. Et comme on a montré que $M_{x,y}$ et $M_{x',y'}$ sont inversibles, leur produit l'est également. Donc

$M_{x,y}M_{x',y'} \neq 0_2$ et finalement $M_{x,y}M_{x',y'} \in G^*$.
• La matrice identité appartient à G^* car $I_2 = M_{1,0}$.
• On a montré à la question précédente que tout élément de G^* est inversible. Et son inverse est encore un élément de G^* car $M_{x,y}^{-1} = M_{\frac{x}{x^2+y^2},-\frac{y}{x^2+y^2}}$.

Nous avons ainsi bien montré que G^* est un sous-groupe de $(\mathrm{GL}_2(\mathbf{R}), \times)$.

2. **Isomorphisme entre $\mathbf{C}^*$ et G^***
On définit l'application

$$\begin{array}{rccc} f: & G^* & \to & \mathbf{C}^* \\ & M_{x,y} & \mapsto & x+\mathrm{i}y. \end{array}$$

(a) Montrer que f est un morphisme de groupe de $(G^*, \times)$ vers $(\mathbf{C}^*, \times)$.

Soient $M = M_{x,y}$ et $M' = M_{x',y'}$ dans G^*. Alors, d'après la question 1.a, $MM' = M_{xx'-yy',xy'+x'y}$. Donc

$$f(MM') = f(M_{xx'-yy',xy'+x'y}) = xx' - yy' + \mathrm{i}(xy' + x'y).$$

D'autre part,

$$f(M)f(M') = (x+\mathrm{i}y)(x'+\mathrm{i}y') = xx' - yy' + \mathrm{i}(xy' + x'y).$$

Finalement, nous avons vérifié que $f(MM') = f(M)f(M')$. Donc f est bien un morphisme de groupe.

(b) Déterminer son noyau.

Soit $M = M_{x,y} \in G^*$. Alors

$$M \in \mathrm{Ker}(f) \text{ ssi } f(M) = 1 \text{ ssi } x + \mathrm{i}y = 1 \text{ ssi } (x,y) = (1,0) \text{ ssi } M_{x,y} = I_2.$$

Donc $\mathrm{Ker}(f) = \{I_2\}$.

(c) Montrer que f est bijectif.

D'après la question précédente, le noyau de f est réduit à un seul élément. On en déduit que f est injectif. D'autre part, f est surjectif par définition de G^*. En effet

$$f(G^*) = \{f(M_{x,y}) \ ; \ (x,y) \in \mathbf{R}^2 \setminus \{(0,0)\}\} = \{x+\mathrm{i}y \ ; \ (x,y) \in \mathbf{R}^2 \setminus \{(0,0)\}\} = \mathbf{C}^*.$$

On conclut que f est bijectif et définit donc un isomorphisme entre G^* et $\mathbf{C}^*$.

3. **Applications**
L'isomorphisme f permet de lier algébriquement les nombres complexes à leurs matrices correspondantes. Pour chacune des questions matricielles suivantes, on pourra commencer par se ramener au problème de nombres complexes correspondant grâce à l'isomorphisme f.

(a) Trouver une matrice A telle que $A^2 = \begin{bmatrix} 3 & -4 \\ 4 & 3 \end{bmatrix}$.

Notons $M = \begin{bmatrix} 3 & -4 \\ 4 & 3 \end{bmatrix}$. Alors $f(M) = 3 + 4\mathrm{i}$. Soit $A \in G^*$. Alors, comme f est un isomorphisme,

$$A^2 = M \text{ ssi } f(A^2) = f(M) \text{ ssi } f(A)^2 = 3 + 4\mathrm{i}.$$

Autrement dit, une matrice A de G^* est une racine carrée de M si et seulement si le nombre complexe associé à A est une racine carrée de $3+4\mathrm{i}$.

Cherchons donc une racine carrée $z = x + \mathrm{i}y$ de $3+4\mathrm{i}$. Cela revient à résoudre le système $x^2 - y^2 = 3$, $2xy = 4$ auquel on ajoute l'égalité des modules $x^2 + y^2 = 5$. On obtient les solutions $z = 2 + \mathrm{i}$ et $-z$.

En particulier, la matrice $A = f(z) = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$ est solution du problème : $A^2 = M$.

Remarque : A et $-A$ ne sont pas les seules racines carrées de M. On peut en trouver d'autres mais elles n'appartiendront pas à G^*.

(b) Trouver une matrice B non diagonale telle que $B^5 = I_2$.

La matrice I_2 est l'image par f du nombre complexe 1. Avec le même raisonnement que précédemment, on montre que pour $B \in G^*$, $B^5 = I_2$ si et seulement si $f(B)^5 = 1$. Le problème revient donc à trouver une racine cinquième de 1. Les racines cinquièmes de 1 sont les nombres de la forme $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{5}}$ avec $k \in \{0,1,2,3,4\}$. On peut prendre par exemple $z = \mathrm{e}^{\frac{2\mathrm{i}\pi}{5}} = \cos(\frac{2\pi}{5}) + \mathrm{i}\sin(\frac{2\pi}{5})$.

Alors en posant $B = f^{-1}(z) = \begin{bmatrix} \cos(\frac{2\pi}{5}) & -\sin(\frac{2\pi}{5}) \\ \sin(\frac{2\pi}{5}) & \cos(\frac{2\pi}{5}) \end{bmatrix}$, B est une matrice non diagonale vérifiant $B^5 = I_2$.

(c) Soit $C = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. Calculer C^{123}.

La matrice C correspond au nombre complexe $z = 1 + \mathrm{i}$. Calculer les puissances de C revient à calculer les puissances de z. Écrivons z sous forme polaire : $z = \sqrt{2}\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$. Alors $z^{123} = \sqrt{2}^{123}\mathrm{e}^{\mathrm{i}\frac{123\pi}{4}} = 2^{61}\sqrt{2}\mathrm{e}^{\mathrm{i}\frac{3\pi}{4}} = -2^{61} + 2^{61}\mathrm{i}$. On en déduit

$$C^{123} = f^{-1}(z)^{123} = f^{-1}(z^{123}) = f(-2^{61} + 2^{61}\mathrm{i}) = \begin{bmatrix} -2^{61} & -2^{61} \\ 2^{61} & -2^{61} \end{bmatrix}.$$

4. **Extension de G^***

Soit $S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Nous souhaitons ajouter S au groupe G^*.

(a) Soit $M = M_{x,y} \in G^*$. Calculer $N = SMS$.

On obtient $N = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$.

(b) Quelle relation simple y a-t-il entre les nombres complexes $f(M)$ et $f(N)$?

La matrice M est associée au nombre complexe $x+\mathrm{i}y$: $f(M) = x+\mathrm{i}y$. La matrice N est elle associée à $x-\mathrm{i}y$: $f(N) = x-\mathrm{i}y$. Ces deux nombres complexes sont conjugués. Donc $f(N) = \overline{f(M)}$.

(c) Déterminer le sous-groupe H de $\mathrm{GL}_2(\mathbf{R})$ engendré par $G^* \cup \{S\}$.
On pourra commencer par calculer S^{-1}, $SM_{x,y}$ et $M_{x,y}S$ et conjecturer les expressions des éléments de H.

Le groupe engendré par les éléments de G^* et S est l'ensemble des matrices que l'on peut obtenir en multipliant entre eux des éléments de G^*, S et S^{-1}. Or $S^{-1} = S$ et on en déduit aussi que pour tout $k \in \mathbf{N}$, $S^k = S$ ou I_2 selon la parité de k.

Calculons les produits d'éléments de G^* avec S : $SM_{x,y} = \begin{bmatrix} x & -y \\ -y & -x \end{bmatrix}$ et $M_{x,y}S = \begin{bmatrix} x & y \\ y & -x \end{bmatrix}$. Notons qu'il ne s'agit pas d'éléments de G^*. Ces deux matrices sont de la forme $\begin{bmatrix} a & b \\ b & -a \end{bmatrix}$, c'est-à-dire symétriques avec des termes diagonaux opposés.
Si on multiplie de nouveau ces matrices par S (à droite ou à gauche), on obtient de nouveau un élément de G^* comme on l'a vu dans la question a. On peut conjecturer qu'il est impossible d'obtenir d'autres matrices que celles de G^* et ces nouvelles matrices. Nous conjecturons donc que

$$H = G^* \cup \left\{ \begin{bmatrix} x & y \\ y & -x \end{bmatrix} \ ; \ (x,y) \in \mathbf{R}^2 \setminus \{(0,0)\} \right\}.$$

Pour le démontrer, remarquons déjà que nous avons justifié que tout élément de cet ensemble est bien engendré par $G^* \cup \{S\}$: les éléments de G^* le sont trivialement et les matrices de la forme $\begin{bmatrix} x & y \\ y & -x \end{bmatrix}$ s'obtiennent par un produit d'un élément $M_{x,y} \in G^*$ avec S. On en déduit que cet ensemble est bien inclus dans H.
Pour conclure, il reste à démontrer que cet ensemble forme un sous-groupe de $(\mathrm{GL}_2(\mathbf{R}), \times)$. Nous laissons le lecteur terminer cela.

(d) Expliquer comment les éléments de H peuvent être mis en correspondance avec certaines transformations géométriques du plan.

Essayons de comprendre ce que nous avons voulu faire en ajoutant S. Nous savons déjà que les éléments de G^* représentent des nombres complexes. Ceux-ci permettent de définir des transformations géométriques du plan : multiplier par un nombre complexe de module 1 revient à effectuer une rotation de centre O, multiplier par un réel revient à multiplier par une homothétie de centre O. Finalement un nombre complexe non nul quelconque permet de définir une similitude centre O (c'est-à-dire une rotation-homothétie).
Nous avons vu à la question b. que la matrice S pouvait permettre de définir une conjugaison des complexes. Celle-ci est naturellement associée à la symétrie d'axe réel. En ajoutant S, on souhaite en fait ajouter toutes les symétries d'axe passant par O. Et c'est bien le cas : une telle symétrie est définie par une application de la forme $z \mapsto \mathrm{e}^{2\mathrm{i}\theta}\bar{z}$ est peut être vue comme la composée de cette symétrie et d'une rotation. Ainsi, si $x + \mathrm{i}y = \mathrm{e}^{2\mathrm{i}\theta}$, la matrice $SM_{x,y}$ permet de définir cette symétrie. Et les matrices de la forme $SM_{x,y} = \begin{bmatrix} x & y \\ y & -x \end{bmatrix}$ permettent de définir toute les composées d'une symétrie et d'une homothétie.

Finalement, pour $a + \mathrm{i}b = r\mathrm{e}^{\mathrm{i}\theta}$, la matrice $M_{a,b} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ peut être associée à la rotation-homothétie d'angle θ, de rapport r. Elle est réalisée par l'application $M_{x,y} \mapsto M_{a,b}M_{x,y}$ qui via f correspond bien à $z \mapsto (a + \mathrm{i}b)z$.
Et la matrice $S_{a,b} = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$ peut être associée à la symétrie-homothétie de rapport r, par rapport à la droite d'angle $\theta/2$. Elle est réalisée par l'application $M_{x,y} \mapsto S_{a,b}M_{x,y}S$ qui correspond à $z \mapsto (a + \mathrm{i}b)\bar{z}$.