

Problème 1 : anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Notations :

- * Pour un ensemble fini F , on note $\text{card}(F)$ son cardinal.
- * Pour $n \in \mathbb{N}$ tel que $n > 1$, on note \mathcal{I}_n l'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ et \mathcal{N}_n l'ensemble des éléments non inversibles.
- * Pour a et $b \in \mathbb{Z}$, " a divise b " est noté $a|b$, ce qui équivaut à : $\exists k \in \mathbb{Z}, b = ka$.
- * Pour a et $b \in \mathbb{Z}$, le plus grand commun diviseur dans \mathbb{N} de a et b est noté $a \wedge b$.
- * Pour $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on désigne par \bar{a} la classe de a dans l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$.

Rappels : on considère (G, \cdot) un groupe fini d'élément neutre 1_G .

- * Soit $a \in G$. On appelle ordre de a , que l'on note $\omega(a)$, le plus petit élément de l'ensemble $\{k \in \mathbb{N}^* / a^k = 1_G\}$.
On a alors : $0 < \omega(a) \leq \text{card}(G)$ et $a^{\omega(a)} = 1_G$.
- * Le groupe G est cyclique si et seulement si il existe $a \in G$ tel que $\text{card}(G) = \omega(a)$.

Éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

1. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $n > 1$. Démontrer que \bar{a} est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si et seulement si $a \wedge n = 1$.
2. Soit $n \in \mathbb{N}$ tel que $n > 1$. Montrer que (\mathcal{I}_n, \times) est un groupe commutatif.
3. Sans justification, énumérer, dans un tableau ayant deux rangées, les éléments de \mathcal{I}_{10} avec leurs ordres. Ce groupe $(\mathcal{I}_{10}, \times)$ est-il cyclique ?
4. Sans justification, énumérer, dans un tableau ayant deux rangées, les éléments de \mathcal{I}_{12} avec leurs ordres. Ce groupe $(\mathcal{I}_{12}, \times)$ est-il cyclique ?
5. Pour les algorithmes demandés, on utilisera uniquement les opérations $\times, +, \wedge$ et la fonction de deux variables **reste** où **reste(a,b)** donne le reste de la division euclidienne de a par b pour $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

On pourra également utiliser des boucles de type

- **for**
- **while**
- et la construction **if...then...else...**

On précisera le logiciel de calcul formel ou le modèle de calculatrice utilisé.

- 5.1. Écrire une procédure **Test**(,) ayant comme arguments deux entiers naturels k et n avec $n > 1$ affichant "1" si $\bar{k} \in \mathcal{I}_n$ et "0" sinon.
- 5.2. Écrire une procédure **Card**() ayant comme argument un entier n avec $n > 1$ affichant le cardinal de \mathcal{I}_n .
- 5.3. Écrire une procédure **Ord**(,) ayant comme arguments deux entiers naturels k et n avec $n > 1$ affichant la valeur de $\omega(\bar{k})$, l'ordre de \bar{k} dans (\mathcal{I}_n, \times) , si $\bar{k} \in \mathcal{I}_n$ et "Erreur" sinon.

Éléments non inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Soit $n \in \mathbb{N}$. On dit que n est primaire lorsqu'il existe un nombre premier p et $\alpha \in \mathbb{N}^*$ tels que $n = p^\alpha$.

6. Soit $n \in \mathbb{N}$ tel que $n > 1$ et n ne soit pas primaire.
 - 6.1. Établir qu'il existe deux entiers, que l'on notera n_1 et n_2 , tels que $n = n_1 n_2$, $1 < n_1 < n$ et $n_1 \wedge n_2 = 1$.
On pourra utiliser la décomposition en produit de facteurs premiers de n .
 - 6.2. Montrer alors que $(n_1 + n_2) \wedge n = 1$.

- 6.3. Établir également que : $\overline{n_1} \notin \mathcal{I}_n$ et $\overline{n_2} \notin \mathcal{I}_n$
7. On considère p un nombre premier et $\alpha \in \mathbb{N}^*$.
Soit $k \in \mathbb{Z}$. Prouver que : $\overline{k} \in \mathcal{N}_{p^\alpha} \iff p|k$.
8. Soit $n \in \mathbb{N}$ tel que $n > 1$.
Démontrer que \mathcal{N}_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si n est primaire.

Problème 2 : isométries du plan et de l'espace

On considère $E = \mathbb{R}^n$ (avec $n \in \{2, 3\}$) muni de sa structure canonique d'espace vectoriel euclidien.
Rappels et notations :

- Pour un ensemble fini F , on note $\text{card}(F)$ son cardinal.
- E est muni canoniquement d'une structure affine.
- Une application affine de E est une application $f : E \rightarrow E$ telle qu'il existe une application linéaire $\varphi : E \rightarrow E$ vérifiant : pour tout $(A, B) \in E^2$, $\overrightarrow{f(A)f(B)} = \varphi(\overrightarrow{AB})$.
 f étant donnée, l'application φ est unique, elle est appelée *partie linéaire* de f et on la note \overrightarrow{f} .
- Une isométrie de E est une application $f : E \rightarrow E$ vérifiant :

$$\text{pour tout } (A, B) \in E^2, \quad f(A)f(B) = AB$$

- Une isométrie de E est une application affine de E .
- Si f est une isométrie de E , on dit que f est un déplacement de E lorsque $\det(\overrightarrow{f}) > 0$.
- On note $Is(E)$ l'ensemble des isométries de E , $Is^+(E)$ l'ensemble des déplacements et $Is^-(E) = Is(E) \setminus Is^+(E)$.
- L'image d'une droite (resp. d'un plan) de E par une isométrie de E est une droite (resp. un plan).
- Une isométrie de E est une bijection de E sur E .
- $(Is(E), \circ)$ est un groupe et $Is^+(E)$ est un sous-groupe de $(Is(E), \circ)$.
- Si $f \in Is^-(E)$ et $g \in Is^-(E)$, alors $f \circ g \in Is^+(E)$.
- Si $f \in Is^+(E)$ et $g \in Is^-(E)$, alors $f \circ g \in Is^-(E)$.
- Pour une isométrie f de E , on note $f^0 = \text{Id}_E$ l'application identité de E , $f^1 = f$, $f^2 = f \circ f$ et f^{-1} la bijection réciproque de f .
- On considère F une partie non vide de E . On note $G(F)$ (respectivement $G^+(F)$) l'ensemble des isométries (respectivement déplacements) de E laissant globalement invariant l'ensemble F .
Ainsi pour tout $f \in Is(E)$ on a : $f \in G(F) \iff f(F) = F$.
De plus, on a : $G^+(F) = G(F) \cap Is^+(E)$.
On définit enfin $G^-(F) = G(F) \setminus G^+(F)$.

Partie A : généralités

1. Soit $f \in Is(E)$.

Établir que $f \in G(F)$ si et seulement si pour tout $M \in F$, on a $\begin{cases} f(M) \in F \\ f^{-1}(M) \in F \end{cases}$.

2. Montrer que $G(F)$ et $G^+(F)$ sont des sous-groupes de $(Is(E), \circ)$.

3. Soit $s \in Is(E)$ telle que s soit une symétrie.

Établir que $s \in G(F)$ si et seulement si pour tout $M \in F$, on a $s(M) \in F$.

On rappelle qu'une symétrie σ de E est une application affine telle que $\sigma \circ \sigma = \text{Id}_E$.

4. On suppose qu'il existe $\varphi \in G^-(F)$. On note $\Phi : \begin{cases} G^+(F) & \longrightarrow & G^-(F) \\ f & \longmapsto & \varphi \circ f \end{cases}$.

4.1. Justifier que Φ est une application bien définie.

4.2. Montrer que Φ est une bijection.

5. Démontrer que si $G(F)$ est fini alors $\text{card}(G(F)) = \text{card}(G^+(F))$ ou $\text{card}(G(F)) = 2 \text{card}(G^+(F))$.

Partie B : exemples dans le plan euclidien

Dans cette partie, on se place dans le cas où $n = 2$ et on désigne par \mathcal{P} le plan \mathbb{R}^2 orienté.

On rappelle que $Is^+(\mathcal{P})$ est constitué des rotations et des translations et que les réflexions (symétries orthogonales par rapport à des droites) sont des éléments de $Is^-(\mathcal{P})$.

Un singleton

Soit Ω un point du plan \mathcal{P} .

1. On considère une application $f \in Is^-(\mathcal{P})$ telle que $f(\Omega) = \Omega$.

1.1. Justifier qu'il existe $I \in \mathcal{P}$ tel que $f(I) \neq I$. On appelle r la réflexion ayant pour axe la médiatrice de $[I, f(I)]$.

1.2. Montrer que $r(\Omega) = \Omega$ puis que $r \circ f = \text{Id}_{\mathcal{P}}$.

1.3. En déduire que f est une réflexion.

2. Démontrer que les éléments de $G(\{\Omega\})$ sont les rotations de centre Ω et les réflexions d'axe passant par Ω .

Une paire

On considère une paire de points du plan, $\mathcal{U} = \{P_1, P_2\}$ où $P_1 \neq P_2$.

On note I le milieu du segment $[P_1, P_2]$.

3. Soit $f \in G(\mathcal{U})$. Montrer que $f(I) = I$.

4. Soit $f \in G^+(\mathcal{U})$ tel que $f \neq \text{Id}_{\mathcal{P}}$. Prouver que f est la symétrie centrale de centre I .

5. Montrer alors que $G(\mathcal{U})$ est formé de quatre éléments : $\text{Id}_{\mathcal{P}}$, la symétrie centrale de centre I et deux réflexions.

Une ellipse

On munit le plan \mathcal{P} d'un repère orthonormé direct $(O; \vec{i}, \vec{j})$. Les axes de coordonnées sont notés : (Ox) et (Oy) .

On considère l'ellipse Γ d'équation : $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ avec $0 < b < a$.

On note $A(a, 0)$ et $A'(-a, 0)$ les sommets principaux de l'ellipse Γ . On note s la symétrie centrale de centre O , r_1 la réflexion d'axe (Ox) et r_2 la réflexion d'axe (Oy) , de sorte que, d'après de qui précède :

$$G(\{A, A'\}) = \{\text{Id}_{\mathcal{P}}, s, r_1, r_2\}$$

6. Soit $M \in \mathcal{P}$ de coordonnées (x, y) . Donner les coordonnées des points $s(M)$, $r_1(M)$ et $r_2(M)$.

7. Montrer alors que $G(\{A, A'\}) \subset G(\Gamma)$.

On note $\Delta = \{M \in \mathcal{P} / OM \leq a\}$ le disque fermé de centre O et de rayon a et Λ le cercle de centre O et de rayon a .

8. Pour $a = \sqrt{3}$ et $b = 1$, représenter sur un même graphique l'ellipse Γ et le cercle Λ .

9. Établir que $\Gamma \subset \Delta$.

10. Montrer que $\Gamma \cap \Lambda = \{A, A'\}$.

11. Soient P et P' deux points de Γ .

(a) Montrer que : $PP' \leq 2a$.

(b) Établir de plus que : $PP' = 2a \iff \{P, P'\} = \{A, A'\}$.

12. En déduire que : $G(\Gamma) = G(\{A, A'\})$.

Partie C : étude d'isométries de l'espace

Pour la fin du problème, on se place dans le cas où $n = 3$. On désigne par \mathcal{E} l'espace \mathbb{R}^3 orienté muni d'un repère orthonormé direct : $\mathcal{R} = (O; \vec{i}, \vec{j}, \vec{k})$. Les axes de coordonnées sont notés (Ox) , (Oy) et (Oz) .

On rappelle qu'un automorphisme u de \mathcal{E} est orthogonal si et seulement si pour tout $\vec{x} \in \mathcal{E}$: $\|u(\vec{x})\| = \|\vec{x}\|$ où $\|\cdot\|$ désigne la norme euclidienne de \mathcal{E} .

$O(\mathcal{E})$ désigne l'ensemble des automorphismes orthogonaux de \mathcal{E} .

On rappelle qu'une matrice $A \in \mathcal{M}_3(\mathbb{R})$ est orthogonale si et seulement si ${}^tAA = I_3 = A{}^tA$ où tA désigne la transposée de la matrice A .

L'ensemble des matrices orthogonales (resp. orthogonales de déterminant 1) est noté $O_3(\mathbb{R})$ (resp. $SO_3(\mathbb{R})$).

1. Soit $f \in Is(\mathcal{E})$.

1.1. Montrer que $\vec{f} \in O(\mathcal{E})$.

On note alors A la matrice de \vec{f} dans la base orthonormale directe $(\vec{i}, \vec{j}, \vec{k})$, X, X' et B les matrices colonnes respectives des coordonnées des points $M(x, y, z)$, $M'(x', y', z')$ et $f(O)(\alpha, \beta, \gamma)$ dans le repère \mathcal{R} .

1.2. Montrer que : $f(M) = M' \iff X' = AX + B$.

(C'est l'expression analytique de f relativement au repère \mathcal{R} .)

1.3. Montrer que : $A \in O_3(\mathbb{R})$ puis que : $f \in Is^+(\mathcal{E})$ si et seulement si $A \in SO_3(\mathbb{R})$.

Pour $i \in \{0, 1, 2, 3\}$ on considère les matrices carrées :

$$A_0 = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, A_1 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ et } A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

2. Justifier que pour $i \in \{0, 1, 2, 3\}$, on a $A_i \in O_3(\mathbb{R})$.

3. Pour quelles valeurs de $i \in \{0, 1, 2, 3\}$, a-t-on $A_i \in SO_3(\mathbb{R})$?

Soit $\lambda \in \mathbb{R}$. On considère la matrice colonne $B_\lambda = \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix}$ et on définit les applications t_λ, v_λ, s et r de \mathcal{E} dans \mathcal{E} par leur expression analytique :

$$t_\lambda : X' = X + B_\lambda, \quad v_\lambda : X' = A_1X + B_\lambda, \quad s : X' = A_2X, \quad r : X' = A_3X$$

De plus, on note $v = v_0$.

On rappelle que $Is^+(\mathcal{E})$ est constitué des translations, des rotations axiales et des vissages. Les réflexions de \mathcal{E} (symétries orthogonales par rapport à un plan) sont des éléments de $Is^-(\mathcal{E})$.

4. Sans justification, donner la nature des transformations t_λ, v, s et r ainsi que leur(s) élément(s) caractéristique(s).

5. Montrer que $v_\lambda = v \circ t_\lambda = t_\lambda \circ v$ et reconnaître cette transformation en précisant ses éléments caractéristiques.

On pourra utiliser un calcul matriciel.

6. Soient γ et $\delta \in \mathbb{R}$. Montrer que $v_\gamma \circ v_\delta = t_{\gamma+\delta}$ et que $t_\gamma \circ v_\delta = v_{\gamma+\delta}$.

Partie D : un cylindre à base elliptique

On considère deux réels strictement positifs a et b tels que $a > b$.

On considère le cylindre \mathcal{C} d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$

On considère Π le plan d'équation $z = 0$ et Γ l'intersection du cylindre \mathcal{C} et du plan Π .

On remarque que la courbe Γ est l'ellipse d'équation : $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ dans $(O; \vec{i}, \vec{j})$ repère orthonormé du plan Π .

Pour $\theta \in \mathbb{R}$ fixé, on considère la droite d_θ de \mathcal{E} d'équations : $\begin{cases} x = a \cos(\theta) \\ y = b \sin(\theta) \end{cases}$.

On va montrer que les éléments de $G(\mathcal{C})$ peuvent s'écrire en composant certaines isométries de la partie précédente.

1. Soit $\lambda \in \mathbb{R}$. Montrer que t_λ, v_λ, s et r sont des éléments de $G(\mathcal{C})$.
2. Montrer que $\mathcal{C} = \bigcup_{\theta \in \mathbb{R}} d_\theta$.
3. Soit \mathcal{D} une droite non parallèle à d_0 .
 - 3.1. Établir que \mathcal{D} admet un vecteur directeur $\vec{u}(\alpha, \beta, \gamma)$ tel que α et β ne sont pas simultanément nuls.
On pourra commencer par donner un vecteur directeur de d_θ pour $\theta \in \mathbb{R}$.
 - 3.2. On note $M_0(x_0, y_0, z_0)$ un point de \mathcal{D} .
Donner une équation paramétrique de la droite \mathcal{D} obtenue à l'aide de \vec{u} et de M_0 .
 - 3.3. Montrer alors que \mathcal{D} coupe \mathcal{C} en au plus deux points.
4. Soit $f \in G(\mathcal{C})$. Dédire de la question précédente que $f(d_0)$ est parallèle à la droite d_0 .
5. Soit $f \in G(\mathcal{C})$. Montrer que \vec{k} est un vecteur propre de \vec{f} .
6. Soit $\varphi \in O(\mathcal{E})$ admettant \vec{k} comme vecteur propre.
 - 6.1. Établir que φ admet dans la base $(\vec{i}, \vec{j}, \vec{k})$ une matrice de $O_3(\mathbb{R})$, donnée par blocs, de la forme $\begin{pmatrix} M & 0 \\ 0 & \varepsilon \end{pmatrix}$ où $M \in O_2(\mathbb{R})$ et $\varepsilon \in \{-1, 1\}$.
 - 6.2. Vérifier que $\varepsilon = \det(\varphi) \det(M)$.
7. Soit $f \in G^+(\mathcal{C})$ tel que $f(O) \in \Pi$. On admet que $f(\Pi) = \Pi$.
On peut donc définir $g : \begin{cases} \Pi \longrightarrow \Pi \\ M \longmapsto g(M) = f(M) \end{cases}$, application induite par f sur Π .
 - 7.1. Établir que g est une isométrie de Π vérifiant $g(\Gamma) = \Gamma$.
 - 7.2. À l'aide de la partie B, énoncer les quatre possibilités pour g puis en déduire que $f(O) = O$.
 - 7.3. Écrire les quatre possibilités pour la matrice de \vec{g} dans la base (\vec{i}, \vec{j}) .
 - 7.4. Vérifier alors que l'on peut trouver i et $j \in \{0, 1\}$ tels que $f = v^j \circ s^i$.
On pourra utiliser l'expression analytique de f et la question 6.
8. Soit $f \in G^+(\mathcal{C})$ tel que $f(O) \notin \Pi$.
On note O' le projeté orthogonal de $f(O)$ sur le plan Π , t la translation de vecteur $\overrightarrow{f(O)O'}$ et $h = t \circ f$.
 - 8.1. Montrer que $h \in G^+(\mathcal{C})$ et $h(O) \in \Pi$.
On pourra commencer par justifier que t peut s'écrire $t = t_\mu$ avec $\mu \in \mathbb{R}^$ et utiliser la question 1.*
 - 8.2. Montrer que l'on peut trouver $\lambda \in \mathbb{R}^*$, i et $j \in \{0, 1\}$ tels que $f = t_\lambda \circ v^j \circ s^i$.
9. Soit $f \in G^-(\mathcal{C})$.
 - 9.1. Établir que $r \circ f \in G^+(\mathcal{C})$.
 - 9.2. En déduire qu'il existe $\lambda \in \mathbb{R}$, i et $j \in \{0, 1\}$ tels que $f = r \circ t_\lambda \circ v^j \circ s^i$.

Partie E : une hélice.

On reprend dans cette partie les notations de la partie précédente.

On considère l'arc paramétré $M : \begin{cases} \mathbb{R} & \longrightarrow & \mathcal{E} \\ t & \longmapsto & M(t) (a \cos(t), b \sin(t), t) \end{cases}$

On note \mathcal{H} la trajectoire de cet arc paramétré.

1. Montrer que $\mathcal{H} \subset \mathcal{C}$.
2. Soit \mathcal{D} une droite telle que \mathcal{D} coupe la courbe \mathcal{H} en au moins trois points.
Montrer alors qu'il existe $\theta \in \mathbb{R}$ tel que $\mathcal{D} = d_\theta$.
On pourra utiliser les questions 2. et 3. de la partie D.
3. Soit $\theta \in \mathbb{R}$. Montrer que $d_\theta \cap \mathcal{H} = \{M(\theta + 2k\pi) / k \in \mathbb{Z}\}$.
4. Soient $f \in G(\mathcal{H})$ et $\theta \in \mathbb{R}$. Montrer qu'il existe $\omega \in \mathbb{R}$ tel que $f(d_\theta) = d_\omega$.
5. En déduire que $G(\mathcal{H}) \subset G(\mathcal{C})$.
6. Soit $k \in \mathbb{Z}$. Montrer que $t_{2k\pi} \in G(\mathcal{H})$.
7. Soit $\lambda \in \mathbb{R}$ tel que $t_\lambda \in G(\mathcal{H})$. Prouver qu'il existe $k \in \mathbb{Z}$ tel que $\lambda = 2k\pi$.
On pourra utiliser le fait que $t_\lambda(M(0)) \in \mathcal{H}$.
8. Justifier brièvement que s et $v_{-\pi} \in G(\mathcal{H})$.
9. Soit $\lambda \in \mathbb{R}$ tel que $v_\lambda \in G(\mathcal{H})$. Prouver qu'il existe $k \in \mathbb{Z}$ tel que $\lambda = (2k + 1)\pi$.
On pourra utiliser le fait que $v_\lambda(M(0)) \in \mathcal{H}$.
10. Soit f une isométrie de \mathcal{E} . Démontrer que :

$$f \in G^+(\mathcal{H}) \iff \exists k \in \mathbb{Z}, \exists i \in \{0, 1\}, \begin{cases} f = t_{2k\pi} \circ s^i \\ \text{ou} \\ f = v_{(2k+1)\pi} \circ s^i \end{cases}$$

11. On veut montrer que $G(\mathcal{H}) = G^+(\mathcal{H})$.
Pour cela, on suppose que $G(\mathcal{H}) \neq G^+(\mathcal{H})$.
 - 11.1. Démontrer qu'il existe $\lambda \in \mathbb{R}$, i et $j \in \{0, 1\}$ tels que $r \circ t_\lambda \circ v^j \circ s^i \in G^-(\mathcal{H})$.
 - 11.2. En déduire que l'on peut trouver un réel noté μ tel que $r \circ t_\mu \in G^-(\mathcal{H})$.
 - 11.3. Calculer les coordonnées du point $r \circ t_\mu(M(0))$.
 - 11.4. En déduire que l'on peut trouver $m \in \mathbb{Z}$ tel que $r \circ t_{2m\pi} \in G^-(\mathcal{H})$.
 - 11.5. En déduire que $r \in G^-(\mathcal{H})$.
 - 11.6. Calculer les coordonnées du point $r\left(M\left(\frac{\pi}{2}\right)\right)$.
 - 11.7. Conclure.