Université Lyon 1

2009/2010

S.P.

Corrigé de l'Ecrit 2. Année 2004.

(Epreuve blanche d'octobre 2009)

Préliminaires:

1. - Si $a \in \bigcap_{i\in I} A_i$ on a pour tout $i \in I$, $f(a) \in f(A_i)$ i.e. $f(a) \in \cap_{i\in I} f(A_i)$. Conclusion: quelquesoit $f : \Omega \to \Omega$,

$$f(\bigcap_{i\in I} A_i) \subset \bigcap_{i\in I} f(A_i).$$

Pour l'inclusion inverse: si $a \in \bigcap_{i\in I} f(A_i)$ alors pour tout $i \in I$, il existe $a_i \in A_i$ tel que $a = f(a_i)$. L'application f étant injective, on doit avoir pour tout $(i, j) \in I^2$, $a_i = a_j \in A_j$. D'où

$$a \in f(\bigcap_{j\in I} A_j).$$

Pour la suite de cette question, $\overline{A} = \Omega \setminus A$.

Remarque: La propriété est fausse pour f non injective: en effet, s'il existe $a, a' \in \Omega$ distincts tels que $f(a) = f(a')$, alors $f(\{a\} \cap \overline{\{a\}}) = f(\emptyset) = \emptyset$ mais $f(\{a\}) \cap f(\overline{\{a\}}) \neq \emptyset$ (car il contient $f(a)$).

- On suppose f injective. On a $f(A \setminus B) = f(A \cap \overline{B}) = f(A) \cap f(\overline{B})$. Reste à voir que $f(\overline{B}) = \overline{f(B)}$: pour cela, observer que $E = f(E) = f(B \cup \overline{B}) = f(B) \cup f(\overline{B})$. Et cette réunion est disjointe car $f(B) \cap f(\overline{B}) = f(B \cap \overline{B}) = \emptyset$.

2. Soit $(A_i)_{i\in I}$ une partition de Ω et $f : \Omega \to \Omega$ une bijection. On a $\Omega = f(\Omega) = f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$ et de plus, pour $j \neq i$, $f(A_i) \cap f(A_j) = f(A_i \cap A_j) = f(\emptyset) = \emptyset$. Conclusion: $(f(A_i))_{i\in I}$ est une partition de Ω.

Pour la réciproque, même argument en utilisant cette fois f^{-1}.

Partie I.

1. a) Dans une base orthonormée de premier vecteur l'axe commun des rotations ρ_1 et ρ_2, les matrices $[\rho_1]$ et $[\rho_2]$ sont du type

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\alpha_i) & -sin(\alpha_i) \\ 0 & sin(\alpha_i) & cos(\alpha_i) \end{pmatrix}, i = 1, 2.$$

Celles-ci commutent.

b) Dans une base orthonormée adaptée aux axes orthogonaux on a

$$[\rho_1] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad [\rho_2] = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Clairement elles commutent.

2. a) On suppose $D \neq \Delta$. Soit $\vec{e}$ (resp. $\vec{e}_\Delta$) un vecteur directeur de D (resp. de Δ). Les valeurs propres réelles de tout endomorphisme orthogonal (en particulier ρ) étant 1 ou -1, on doit avoir

$$\rho(\vec{e}_\Delta) = -\vec{e}_\Delta$$

d'où

$$(\vec{e}, \vec{e}_\Delta) = (\rho(\vec{e}), \rho(\vec{e}_\Delta)) = -(\vec{e}, \vec{e}_\Delta),$$

i.e. $(\vec{e}, \vec{e}_\Delta) = 0$.

On sait que les valeurs propres $z \in \mathbf{C} \setminus \mathbf{R}$ d'un endomorphisme réel viennent par paires conjuguées $z, \overline{z}$ (z est racine complexe d'un polynôme à coefficients réels). ρ ayant déjà deux valeurs propres réelles $+1$ et -1, la troisième l'est aussi et vaut $+1$ ou -1. Le déterminant étant le produit des valeurs propres, $Det(\rho) = 1$ implique que cette dernière vaut -1. Dès lors, $E = D \oplus D^\perp$ avec $\rho_{|_{D^\perp}} = -id_{D^\perp}$ et ρ est un demi-tour d'axe D.

b) Soit $\vec{e}_1$ un vecteur directeur de D_1. On a $\rho_1(\rho_2(\vec{e}_1)) = \rho_2(\rho_1(\vec{e}_1)) = \rho_2(\vec{e}_1)$. Dès lors $\rho_2(\vec{e}_1) \in D_1$ i.e. $\rho_2(D_1) = D_1$ (la droite D_1 est globalement invariante mais n'est pas fixe). Idem en permutant 1 et 2. Par le a), ρ_1 et ρ_2 sont des demi-tours d'axes orthogonaux.

c) ρ_1 et ρ_2 ($\neq id$) commutent ssi (1) elles ont même axe ou (2) ce sont des demi-tours d'axes orthogonaux.

3. Dans cette question ρ_1 et ρ_2 sont deux rotations de même axe d'angles respectifs α_1 et α_2.

a) Il est immédiat de voir que H est un sous-groupe de $O(E)^+$. Par définition (cf fiche de cours), le sous-groupe $\langle \rho_1, \rho_2 \rangle$ engendré par ρ_1, ρ_2 est l'ensemble des composées finies de $\rho_1, \rho_2, \rho_1^{-1}, \rho_2^{-1}$. Ici, $\rho_1\rho_2 = \rho_2\rho_1$ et toute composée finie est du type

$$\rho_1^{n_1}\rho_2^{n_2}, \quad n_1, n_2 \in \mathbf{Z},$$

i.e. $H = \langle \rho_1, \rho_2 \rangle$.

b) Le couple (n_1, n_2) existe par déf. du sous-groupe engendré. Maintenant

$$\rho_1^{n_1}\rho_2^{n_2} = \rho_1^{m_1}\rho_2^{m_2} \Leftrightarrow \rho_1^{n_1-m_1}\rho_2^{n_2-m_2} = id$$

i.e. la rotation d'angle $(n_1 - m_1)\alpha_1 + (n_2 - m_2)\alpha_2$ est l'identité i.e. il existe $z \in \mathbf{Z}$ tel que

$$(n_1 - m_1)\alpha_1 + (n_2 - m_2)\alpha_2 = 2\pi z$$

ce qui, par hypothèse, implique $n_1 = m_1, n_2 = m_2, z = 0$.

4. On suppose que ρ_1 et ρ_2 sont deux demi-tours d'axes orthogonaux.

Dans une base orthonormée $(\vec{e}_i)_{1 \leq i \leq 3}$ adaptée aux axes, on a, comme plus haut,

$$[\rho_1] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad [\rho_2] = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

D'où

$$\rho_i^{2n} = id, \quad i = 1, 2,\ n \in \mathbf{N}$$

ce qui s'écrit aussi $\rho_i^{-n} = \rho_i^n$, en particulier on peut se limiter aux composées de ρ_1 et ρ_2. Le seul élément nouveau qui apparait est

$$[\rho_1\rho_2] = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = [\rho_2\rho_1].$$

C'est le demi-tour ρ_3 d'axe $\vec{e}_3$. On a donc

$$\langle \rho_1, \rho_2 \rangle = \{id, \rho_1, \rho_2, \rho_3 = \rho_1\rho_2\}.$$

Je vous laisse la table.

5. Cette question revient à la définition même du sous-groupe $\langle \rho_1, \rho_2 \rangle$ engendré par ρ_1 et ρ_2 qui cette fois ne commutent pas (cf cours).

Deux remarques toutefois:

(1) Il faut veiller à l'ordre des produits, en particulier, le réciproque de $s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}$ est $s_n^{-a_n} s_{n-1}^{-a_{n-1}} \cdots s_2^{-a_2} s_1^{-a_1}$.

(2) Dans la décomposition $g = s_1^{a_1} \cdots s_n^{a_n}$ l'ordre importe mais lorsque $s_i = s_{i+1}$ on regroupe bien sûr les termes successifs en utilisant $s_i^{a_i} s_{i+1}^{a_{i+1}} = s_i^{a_i + a_{i+1}}$ si bien qu'il existe au moins une décomposition de g pour laquelle pour tout i, $s_i \neq s_{i+1}$. (Par exemple $\rho_1\rho_1^2\rho_2\rho_1 = \rho_1^3\rho_2\rho_1, ...$)

Partie II.

1. On suppose $\alpha = arccos\frac{3}{5}$.

a) Pour $n \geq 1$, on a

$$cos(n+1)\alpha + cos(n-1)\alpha = 2\, cosn\alpha\, cos\alpha = \frac{6}{5}\, cosn\alpha.$$

D'où, en multipliant cette égalité par 5^{n+1},

$$a_{n+1} + 25a_{n-1} = 5^{n+1}\,\frac{6}{5}\, cosn\alpha = 6a_n.$$

b) On a $sin\alpha = \pm\sqrt{1 - cos^2\alpha} = \pm\frac{4}{5}$. Mais $\alpha \in [0, \pi]$ implique $sin\alpha = \frac{4}{5}$. (*Ce dernier point montre au moins que vous savez que pour définir l'inverse de cos il faut choisir un domaine où il est monotone (ici décroissant).*)

Pour $n \geq 0$, il vient

$$\begin{aligned} b_{n+1} &= 5^{n+1} sin(n+1)\alpha \\ &= 5^{n+1}(sin\, n\alpha\, cos\alpha + cos\, n\alpha\, sin\alpha) \\ &= 5^{n+1}(\frac{3}{5}\, sin\, n\alpha + \frac{4}{5}\, cosn\alpha) \\ &= 3b_n + 4a_n. \end{aligned}$$

c) Pour $n \geq 0$, par récurrence en observant $a_0 = 1, b_0 = 0, a_1 = 3, b_1 = 4$ et en utilisant a). Pour $n < 0$, observer que $a_n = a_{-n}$.

Démo analogue pour b_n en utilisant b) et $b_{-n} = -b_n$.

d) Il suffit de le faire pour $n \geq 1$. On procède par récurrence: c'est vrai pour a_1. Ensuite utiliser

$$a_{n+1} = 6a_n - 25a_{n-1} \equiv 6a_n[5] \equiv a_n[5] \equiv 3[5].$$

e) Récurrence pour $n > 0$: C'est vrai pour b_1. Pour $n \geq 1$, utiliser

$$b_{n+1} = 3b_n + 4a_n \equiv (12 + 12)[5] \equiv 4[5].$$

$n < 0$: on a

$$b_n = -b_{-n} \equiv -4[5] \equiv 1[5].$$

Remarque: certains étudiants n'observent pas les relations $a_n = a_{-n}$, $b_n = -b_{-n}$ et font une récurrence dans $\mathbf{Z}$ sans préciser $n < 0$ ou $n > 0$. Ce qui conduit à des erreurs dans les congruences du e).

2. a) Soient les matrices $A = (a_{ij})$, $B = (b_{ij}) \in M_3(\mathbf{Z})$. La congruence $A \equiv B$ signifie

$$\text{pour tout } i, j, \quad a_{ij} \equiv b_{ij}[5].$$

Pour montrer $A \equiv B$ et $C \equiv D \Rightarrow AC \equiv BD$ il suffit d'écrire le produit matriciel $AC = (\sum_l a_{il}c_{lj})$ et de rappeler que la congruence modulo $n \in \mathbf{N}$ est compatible avec la somme et le produit d'entiers.

Remarque: pour ce type de questions, une rédaction succincte suffit.

b) 5^0R^0 est la matrice identité. Pour $k > 0$, R^k est la matrice de rotation d'angle $k\alpha$, d'où

$$5^{|k|}R^k = 5^{|k|}\begin{pmatrix} cos\, k\alpha & -sin\, k\alpha & 0 \\ sin\, k\alpha & cos\, k\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_k & -b_k & 0 \\ b_k & a_k & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbf{Z}).$$

Pour $k < 0$, observer que

$$5^{|k|}R^k = 5^{|k|}R^{-|k|} = \begin{pmatrix} a_{|k|} & b_{|k|} & 0 \\ -b_{|k|} & a_{|k|} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbf{Z}).$$

Idem pour T. Les congruences modulo 5 résultent des questions 1 d) et 1 e).

Existe-t-il un entier $k \neq 0$ tel que $R^k = I_3$?

Pour un tel k on aurait

$$5^{|k|}R^k = \begin{pmatrix} 5^{|k|} & 0 & 0 \\ 0 & 5^{|k|} & 0 \\ 0 & 0 & 5^{|k|} \end{pmatrix},$$

ce qui implique $b_k \equiv 0[5]$. Donc, **non** un tel k n'existe pas.
Idem pour T^k.

c) Par le 2.a) on a

$$\begin{aligned} 5^{|m|}T^m 5^{|n|}R^n &\equiv \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & \epsilon_m \\ 0 & -\epsilon_m & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & \epsilon_n & 0 \\ -\epsilon_n & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 & 0 & 0 \\ -3\epsilon_n & 9 & 0 \\ \epsilon_m\epsilon_n & -3\epsilon_m & 0 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 & 0 & 0 \\ 2\epsilon_n & 4 & 0 \\ \epsilon_m\epsilon_n & 2\epsilon_m & 0 \end{pmatrix} \end{aligned}$$

car $-3 \equiv 2[5]$ et $9 \equiv 4[5]$.

d) Pour la forme de la matrice $\begin{pmatrix} 0 & 0 & 0 \\ a & b & 0 \\ c & d & 0 \end{pmatrix}$, procéder par récurrence sur n en observant que pour $n = 1$, cette forme est bien celle du c).

Récurrence aussi pour montrer que les coefficients a, b, c, d ne sont pas multiples de 5: pour $n = 1$, $\epsilon_{a_1}\epsilon_{b_1} = \pm 1$, 4, $2\epsilon_{a_1} = \pm 2$ et $2\epsilon_{a_2} = \pm 2$ ne sont pas multiples de 5. Reste à voir que si les coefficients a, b, c, d obtenus à l'ordre n ne sont pas multiples de 5 alors les coefficients du produit

$$\begin{aligned} &5^q T^{a_1}R^{b_1}\cdots T^{a_n}R^{b_n} \cdot 5^{|a_{n+1}|+|b_{n+1}|}T^{a_{n+1}}R^{b_{n+1}} \\ &\qquad = \begin{pmatrix} 0 & 0 & 0 \\ a & b & 0 \\ c & d & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 2\epsilon_{b_{n+1}} & 4 & 0 \\ \epsilon_{a_{n+1}}\epsilon_{b_{n+1}} & 2\epsilon_{a_{n+1}} & 0 \end{pmatrix} \\ &\qquad = \begin{pmatrix} 0 & 0 & 0 \\ 2b\epsilon_{b_{n+1}} & 4b & 0 \\ 2d\epsilon_{b_{n+1}} & 4d & 0 \end{pmatrix} \end{aligned}$$

ne le sont pas non plus: c'est vrai car, 5 étant premier, il n'y a pas de diviseur de 0 dans $\mathbf{Z}/5\mathbf{Z}$.

e) S'il existait $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbf{Z}^{\star n}$ tels que $T^{a_1}R^{b_1}\cdots T^{a_n}R^{b_n} = I_3$ on aurait $5^q T^{a_1}R^{b_1}\cdots T^{a_n}R^{b_n} \equiv O_3$ ce qui contredit le point d). (Ici, O_3 est la matrice nulle.)

Remarque: certains étudiants écrivent: la matrice $\begin{pmatrix} 0 & 0 & 0 \\ a & b & 0 \\ c & d & 0 \end{pmatrix}$ *n'étant pas inversible elle ne peut être égale à* $5^q I_3$. *Ce raisonnement est faux car la congruence ne préserve pas l'inversibilité.*

Raisonnement analogue pour $T^{a_1}R^{b_1}\cdots T^{a_n}R^{b_n}T^{\beta}\neq I_3$. En effet, on a

$$5^{q+|\beta|}T^{a_1}R^{b_1}\cdots T^{a_n}R^{b_n}T^{\beta}\equiv\begin{pmatrix}0&0&0\\a&b&0\\c&d&0\end{pmatrix}\cdot\begin{pmatrix}0&0&0\\0&3&\epsilon_\beta\\0&-\epsilon_\beta&3\end{pmatrix}$$
$$\equiv\begin{pmatrix}0&0&0\\0&3b&b\epsilon_\beta\\0&3d&d\epsilon_\beta\end{pmatrix}$$

dont les coefficients ne sont pas multiples de 5 (car 5 est premier et $3, b, d, \epsilon$ ne sont pas multiples de 5).

3. S'il existait $(a_1,\ldots,a_n),(b_1,\ldots,b_n)\in\mathbf{Z}^{\star n}$ tels que $R^{a_1}T^{b_1}\cdots R^{a_n}T^{b_n}=I_3$ alors, par inversion, on aurait

$$T^{-b_n}R^{-a_n}\cdots T^{-b_1}R^{-a_1}=I_3$$

ce qui contredit la première inégalité de la question 2 e).

On peut en déduire l'inégalité $R^{a_1}T^{b_1}\cdots R^{a_n}T^{b_n}R^{\beta}\neq I_3$ comme dans 2 e).

4. L'existence d'une telle décomposition (dite réduite) résulte de la définition de $\langle\rho,\tau\rangle$. Pour l'unicité: l'égalité

$$s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n}={s'_1}^{a'_1}{s'_2}^{a'_2}\cdots {s'_{n'}}^{a'_{n'}},\quad n\leq n'$$

équivaut à

$$s_n^{-a_n}\cdots s_1^{-a_1}{s'_1}^{a'_1}{s'_2}^{a'_2}\cdots {s'_{n'}}^{a'_{n'}}=id.$$

Si la partie

$$P=\{j\in\mathbf{N}\setminus\{0\},j\leq\ \min\ n,\ s_j^{-a_j}{s'_j}^{a'_j}\neq id\}$$

était non vide, pour $i=\min\,(P)$, on aurait

$$s_n^{-a_n}\cdots s_{i+1}^{-a_{i+1}}(s_i^{-a_i}{s'_i}^{a'_i}){s'_{i+1}}^{a'_{i+1}}\cdots {s'_{n'}}^{a'_{n'}}=id,$$

ce qui contredit les inégalités des questions 2 et 3. D'où $P=\emptyset$ et on a

$$(\iota)\text{ pour tout } j\leq n,\ s_j^{-a_j}{s'_j}^{a'_j}=id,\qquad(\iota\iota){s'_{n+1}}^{a'_{n+1}}\cdots {s'_{n'}}^{a'_{n'}}=id.$$

Si $n\neq n'$, $(\iota\iota)$ contredit les inégalités des questions 2 et 3. On a donc $n=n'$. Enfin les inégalités de 2, 3 et (ι) impliquent

$$\text{pour tout } 1\leq j\leq n,\quad s_j=s'_j,\ a_j=a'_j.$$

5. Par 4. le groupe G est infini.

Notons $G_0 = \{id\}$. Pour $n \in \mathbf{N} \setminus \{0\}$, considérons l'application

$$w_n : \{\rho, \tau\}^n \times \mathbf{N}^n \to G : \big((s_1, \ldots, s_n), (a_1, \ldots, a_n)\big) \mapsto s_1^{a_1} \cdots s_n^{a_n}$$

et notons $G_n = w_n(\{\rho, \tau\}^n \times \mathbf{N}^n)$. On sait que $\{\rho, \tau\}^n \times \mathbf{N}^n$ est dénombrable (cf fiche sur les dénombrements: tout produit fini de dénombrables est dénombrable) dès lors G_n l'est aussi comme image d'un dénombrable par la surjection w_n. Enfin $G = \bigcup_{n \in \mathbf{N}} G_n$ l'est aussi comme réunion dénombrable de dénombrables.

6. Si $g = s_1^{a_1} \cdots s_n^{a_n}$ est la décomposition de la question 4 de $g \in G \setminus \{id\}$, le terme de tête est défini par $t(g) = s_1$ si $a_1 > 0$ et $t(g) = s_1^{-1}$ si $a_1 < 0$.

On note $L(\sigma) \subset G \setminus \{id\}$ l'ensemble des éléments de G tels que $t(g) = \sigma$, $\sigma \in \{\rho, \rho^{-1}, \tau, \tau^{-1}\}$.

a) L'existence et l'unicité de la décomposition du 4 pour tout élément $g \in G \setminus \{0\}$ nous dit que

$$G = \{id\} \cup L(\rho) \cup L(\rho^{-1}) \cup L(\tau) \cup L(\tau^{-1})$$

est une réunion de parties deux à deux disjointes i.e. détermine une partition de G.

b) L'élément $g = s_1^{a_1} \cdots s_n^{a_n}$ appartient à $L(\rho)$ ssi $a_1 > 0$. On a deux possibilités: (1) $a_1 \geq 2$ auquel cas $g \in \rho L(\rho)$, (2) $a_1 = 1$ et on a l'un des trois cas suivants: $g = \rho$, $g \in \rho L(\tau)$ ou $g \in \rho L(\tau^{-1})$.

D'où

$$L(\rho) = \{\rho\} \cup \rho L(\rho) \cup \rho L(\tau) \cup \rho L(\tau^{-1})$$

détermine une partition de $L(\rho)$.

De même pour

$$L(\rho^{-1}) = \{\rho^{-1}\} \cup \rho^{-1} L(\rho^{-1}) \cup \rho^{-1} L(\tau) \cup \rho^{-1} L(\tau^{-1}).$$

c) Par la seconde décomposition du b) on a

$$\rho L(\rho^{-1}) = \{id\} \cup L(\rho^{-1}) \cup L(\tau) \cup L(\tau^{-1}).$$

Ensuite le a) donne

$$G = L(\rho) \cup \rho L(\rho^{-1}).$$

Idem en remplaçant ρ par τ.

Remarque: bien que sa formulation puisse intimider certains, la question 6. ne demande aucune réflexion. Il s'agit d'un point d'écriture ensembliste.

Partie III.

On désigne par S^2 la sphére unité de $\mathbf{R}^3$.

1. Pour voir que la partie

$$F = \{v \in S^2, |\ \exists g \in G \setminus \{id\}, g(v) = v\}$$

est dénombrable, observer que l'axe de $g \neq id$ intersecte S^2 en deux points $v_+(g), v_-(g) = -v_+(g)$. Dès lors

$$F = \bigcup_{g \in G \setminus \{id\}} \{v_+(g), v_-(g)\}$$

est au plus dénombrable comme réunion dénombrable d'ensembles finis.

Soit $p_+ \in S^2$ le pôle nord. Par projection stéréographique, $S^2 \setminus \{p_+\}$ est en bijection avec le plan $\mathbf{R}^2$ qui n'est pas dénombrable (il contient $\mathbf{R}$). Dès lors S^2 n'est pas dénombrable et $X = S^2 \setminus F$ non plus (en effet, si X était dénombrable, $S^2 = X \cup F$ serait dénombrable comme réunion finie de dénombrables).

2. Soit $v \in X$, $g \in G \setminus \{id\}$. Pour montrer $g(v) \in X$, il suffit d' observer que si on a $g(v) \in F$ i.e. s' il existe $g' \in G \setminus \{id\}$ tel que $g'(g(v)) = v$ alors (par définition) $v \in F$.

3. Soit $g, h \in G \setminus \{id\}$. On suppose qu'il existe $v \in X$ tel que $g(v) = h(v)$ i.e. tel que $(h^{-1}\, g)(v) = v$. Si $h^{-1}\, g \neq id$ on aurait $v \in F$.

4. a) Puisque $G \subset O_3^+$, tout élément $g \in G$ stabilise S^2 i.e. induit une bijection

$$g_{S^2} : S^2 \to S^2 : s \mapsto g(s).$$

Par la question 2, quelquesoit $v \in X$, on a $g(v) \in X$ et $g^{-1}(v) \in X$. Dès lors g_{S^2} induit une bijection

$$g_X : X \to X : v \mapsto g(v).$$

b) Vérifier que $G \to S(X) : g \mapsto g_X$ est un morphisme est un jeu d'écriture: en effet, pour $v \in X$, $(g \circ h)_X(v) = (g \circ h)(v) = g(h(v)) = g_X(h_X(v)) = (g_X \circ h_X)(v)$.

Vérifions qu'elle est injective: $g_X = h_X$ signifie que quelquesoit $v \in X, g(v) = h(v)$. Par la question 3, $g = h$. (En fait la question 3 nous assure de l'égalité sous une condition beaucoup plus faible: il suffit qu'il existe $v \in X$ tel que $h(v) = g(v)$.)

5. Montrer que *la relation sur X définie par $a \sim b \Leftrightarrow \exists g \in G, a = g(b)$ est une équivalence* est une question de cours. Je répète donc:

(1) réflexivité: en prenant $g = id$ on a $a \sim a$.

(2) symétrie: si $a = g(b)$ alors $b = g^{-1}(a)$.

(3) transitivité: si $a = g(b)$ et $b = h(c)$ alors $a = (g\, h)(c)$.

6. Par hypothèse $M \subset X$ intersecte chaque classe (i.e. chaque orbite $O_v = \{g(v), g \in G\}$) en un seul point. On veut montrer que $(g(M))_{g \in G}$ est une partition de X.

Pour $v \in X$ notons $\{v'\} = M \cap O_v$. Par définition de O_v, il existe $g \in G$ tel que $v' = g(v)$. D'où $v = g^{-1}(v') \in g^{-1}(M)$ i.e. on a

$$X = \bigcup_{g \in G} g(M).$$

Reste à voir que les parties $g(M)$ sont deux à deux disjointes: supposons, par l'absurde qu'il existe $g, g' \in G$ distincts tels que

$$g(M) \cap g'(M) \neq \emptyset.$$

Soit $w \in g(M) \cap g'(M)$ et $m, m' \in M \subset X$ tels que $w = g(m) = g'(m')$. L' égalité $m' = ({g'}^{-1}\, g)(m)$ implique $m' \neq m$ (car si $m' = m$, on aurait $m \in F$). La partie M contient donc deux points distincts $m = g^{-1}(w)$ et $m' = {g'}^{-1}(w)$ de l'orbite O_w. Ce qui contredit l'hypothèse faite sur M.

7. a) Il suffit d'utiliser la question qui précède et le 6 a) de la partie II.

b) On a

$$X_1 = \bigcup_{g \in L(\rho)} g(M), \quad X_3 = \bigcup_{g \in L(\rho^{-1})} g(M).$$

D'où

$$\rho(X_3) = \bigcup_{g \in L(\rho^{-1})} (\rho\, g)(M) = \bigcup_{g \in \rho L(\rho^{-1})} g(M)$$

et en utilisant le 6 c) de la partie II et la question qui précède,

$$\begin{aligned} X = \bigcup_{g \in G} g(M) &= \bigcup_{g \in L(\rho) \cup \rho L(\rho^{-1})} g(M) \\ &= X_1 \cup \rho(X_3) \quad \text{(réunion disjointe)}. \end{aligned}$$

Idem pour $X = X_2 \cup \tau(X_4)$.

8. a) $\Lambda = \{(u, v) \in F \times F \mid u \neq v\}$ est au plus dénombrable car $F \times F$ l'est (comme produit fini d'au plus dénombrables).

b) Pour $(u, v) \in \Lambda$, quel est la nature géométrique de

$$\Gamma_{u,v} = \{w \in S^2 \mid || w - u || = || w - v ||\}?$$

u, v étant de norme 1, la condition $|| w - u ||^2 = || w - v ||^2$ s'écrit

$$(w - u, w - u) = (w - v, w - v) \Leftrightarrow -2(w, u) = -2(w, v) \Leftrightarrow (w, u - v) = 0.$$

Le lieu $\Gamma_{u,v}$ est donc l'intersection du plan (vectoriel) médiateur du segment $[u, v]$ avec la sphère S^2. C'est donc un grand cercle de S^2.

c) Soit $\Gamma = \bigcup_{(u,v) \in \Lambda} \Gamma_{u,v}$.

- $\Gamma \cup F$ est symétrique par rapport à l'origine $O = (0, 0, 0)$: pour commencer, F l'est car $g(v) = v \Rightarrow g(-v) = -v$. Ensuite $\Gamma_{u,v}$ l'est car c'est un grand cercle. Conclusion: $\Gamma \cup F$ est symétrique comme réunion d'ensembles symétriques.

- $\Gamma \cup F$ est une partie stricte de S^2: on va utiliser l'indication. Soit $C \subset S^2$ un cercle non centré en l'origine $O = (0, 0, 0)$. Quelquesoit $(u, v) \in \Lambda$, $\Gamma_{u,v}$ étant centré en O, on a $\Gamma_{u,v} \neq C$. Ces deux cercles ont donc au plus 2 points d'intersection. Dès lors

$$\Gamma \cap C = (\bigcup_{(u,v) \in \Lambda} \Gamma_{u,v}) \cap C = \bigcup_{(u,v) \in \Lambda} (\Gamma_{u,v} \cap C)$$

est au plus dénombrable comme réunion dénombrable d'ensembles finis. De même, $F \cap C$ est au plus dénombrable comme partie de l'ensemble au plus dénombrable F. D'où

$$(\Gamma \cup F) \cap C = (\Gamma \cap C) \cup (F \cap C) \text{ est au plus dénombrable.}$$

Conclusion: C ayant la cardinalité de $\mathbf{R}$ on a $(\Gamma \cup F) \cap C \neq C$. A fortiori, $\Gamma \cup F \neq S^2$.

d) L'inclusion stricte du c) assure l'existence d' un point $z \in S^2$ tel que $z \notin \Gamma \cup F$. Par symétrie de $\Gamma \cup F$ on a aussi $-z \notin \Gamma \cup F$.

Soit donc r une rotation d'axe la droite vectorielle $< z >$ et d'angle $2\beta\pi$.

Si $p \in \mathbf{Z}^\star$ est tel que $r^p = id$ alors $2p\beta\pi = 2\pi l$ pour un certain $l \in \mathbf{Z}$ et $\beta \in \mathbf{Q}$.

Conclusion: pour β irrationnel, quelquesoit $p \in \mathbf{Z}^\star$, $r^p \neq id$.

e) Soit $(u, v) \in F \times F$. On veut montrer que pour tout entier $k > 0$, $r^k(u) \neq v$.

Commençons par relire ce qui précède:

par le point d), r^k est une rotation ($\neq id$) d'axe la droite vectorielle $< z >$ avec $z \notin \bigcup_{(u,v)\in\Lambda} \Gamma_{u,v} \cup F$.

cas $u = v$: si pour $k > 0$, on a $r^k(u) = u$ alors $u \in < z > \cap S^2$ i.e. $u = \pm z$ ce qui contredit $z \notin F$.

cas $u \neq v$: on sait que pour toute rotation ρ d'axe $< z >$ et tout point $w \in \mathbf{R}^3$ on a $(\rho(w) - w, z) = 0$. En particulier $(r^k(u) - u, z) = 0$. Si $r^k(u) = v$ on a donc

$$(v - u, z) = 0$$

i.e. z appartient au grand cercle $\Gamma_{u,v}$. Contradiction.

L'identité

$$r^n(F) \cap r^m(F) = \emptyset$$

pour tout entier naturel $n, m, m < n$ en résulte immédiatement:

par l'absurde, si $w \in r^n(F) \cap r^m(F)$, il existe $u, v \in F$ tels que $w = r^n(u) = r^m(v)$ d'où

$$r^{n-m}(u) = v, \quad n - m > 0$$

ce qui contredit ce qui précède.

f) ne contient pas de question.

g) On pose $Y = \bigcup_{n\in\mathbf{N}} r^n(F)$, $Z = S^2 \setminus Y$.

Observer, en utilisant les rappels ensemblistes, que

$$r(Y) = r(\bigcup_{n\in\mathbf{N}} r^n(F)) = \bigcup_{n\in\mathbf{N}} r^{n+1}(F) = \bigcup_{n\in\mathbf{N}\setminus\{0\}} r^n(F) \subset Y.$$

En particulier, $r(Y) \cap Z = \emptyset$.

Reste à vérifier que $S^2 \setminus F = r(Y) \cup Z$.

Par la question e) on a, pour tout entier $n > 0$, $r^n(F) \cap F = \emptyset$ i.e. $r(Y) \subset S^2 \setminus F$. De plus $F = r^0(F) \subset Y$ équivaut à $Z = S^2 \setminus Y \subset S^2 \setminus F$. On a donc $(r(Y) \cup Z) \cap F = \emptyset$.

Pour conclure, observer que

$$S^2 = Y \cup (S^2 \setminus Y) = (F \cup r(Y)) \cup Z = F \cup (r(Y) \cup Z).$$