DEVOIR SURVEILLÉ n° 1 (2H)

Vendredi 9 septembre 2016

I — L'usage des calculatrices est interdit

L'étudiant attachera la plus grande importance à la clarté, à la précision et à la concision de la rédaction, même si tout résultat qui n'est pas explicitement dans le cours de MPSI ou de MP doit être démontré. Si un candidat repére ce qui lui semble être une erreur d'énoncé, il le signalera sur sa copie et poursuivra sa composition en expliquant les raisons des initiatives qu'il a été amené à prendre.

1) Théorème de Lagrange dans un groupe commutatif

Soit $(G, .)$ un groupe multiplicatif, commutatif, fini et de neutre e. Soit $a \in G$.

1. Justifier **rigoureusement** qu'il existe un plus petit entier naturel non nul n_0 (appelé ordre de a) tel que $a^{n_0} = e$.

2. Soit $n \in \mathbb{N}^*$ tel que $a^n = e$. Démontrer que l'ordre de a divise n.

3. Soit $P = \prod_{g \in G} g$. Justifier rapidement que P est un élément de G.

4. Montrer que $f_a : G \to G$ telle que $f_a(g) = a \cdot g$ est une bijection de G dans G.

5. En considérant $\prod_{g \in G} f_a(g)$, montrer que l'ordre de a divise le cardinal de G.

On suppose avoir défini une fonction en langage Python `Mult(a,b)` renvoyant le résultat du produit $a \cdot b$ des éléments a et b dans G. On suppose aussi que la variable `e` contient la valeur du neutre du groupe G.

6. Écrire une fonction `ordre(a)` renvoyant la valeur de l'ordre de a dans G.

2) Opérations ensemblistes sur les sous groupes

Soit $(G, \cdot)$ un groupe. Lorsque A est une partie de G, on note $\overline{A}$ son complémentaire dans G.

1. Énoncer puis démontrer un résultat général concernant l'intersection de deux sous groupes de G.

2. Énoncer puis démontrer un résultat général concernant le produit cartésien de deux (sous) groupes (de G).

3. Justifier que le complémentaire d'un sous groupe de G n'est jamais un sous groupe de G.

4. Justifier que, de manière générale, l'union de deux sous groupes peut ne pas être un sous groupe.

5. Soient H_1 et H_2 deux sous groupes de G tels que :

(•) l'union $H_1 \cup H_2$ est aussi un sous groupe de G

(••) il existe $y \in (H_1 \cap \overline{H_2})$.

a. Soit $x \in H_2$. Justifier que $x \cdot y \in H_1 \cup H_2$, puis montrer que $x \in H_1$.

b. Conclure.

6. En déduire une condition nécessaire sur les sous-groupes H_1 et H_2 pour que l'union $H_1 \cup H_2$ soit un sous-groupe. Démontrer que c'est une condition suffisante.

7. Déterminer deux sous groupes non triviaux de $\mathbb{Z}$ dont l'union est encore un sous groupe de $\mathbb{Z}$.

3) Matrices triangulaires

Soit G l'ensemble des matrice 3×3 de la forme $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ pour x, y et z dans $\mathbb{R}$. On note $\cdot$ la multiplication classique des matrices.

1. Vérifier que $(G, \cdot)$ est un groupe.

2. Soit l'ensemble $\mathbb{R}^2$ muni de la loi $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$.
Vérifier à la main, ou bien justifier rapidement à l'aide d'un résultat du cours, que $(\mathbb{R}^2, +)$ est bien un groupe.

3. Soit f l'application :

$$f : \begin{array}{ccc} (G, \cdot) & \to & (\mathbb{R}^2, +) \\ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} & \mapsto & (x, z) \end{array}$$

Montrer que f est un morphisme de groupe.

4. Déterminer l'image et le noyau de f.

4) Deux groupes non isomorphes

Montrer que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.

5) Les quaternions

Partie 1 : des résultats généraux utiles

1. Soit $(G, \cdot)$ un groupe multiplicatif. Soit X une partie de G. Montrer que le sous-groupe $< X >$ engendré par X est l'ensemble des mots (produits) finis construits sur $X \cup X^{-1}$.

2. On note e le neutre du groupe multiplicatif $(G, \cdot)$. On suppose qu'il existe dans G un élément $g \neq e$ tel que $g^2 = e$.
Soit $x \in G$ tel que $x^2 = g$. Que peut-on dire de l'ordre de x dans G ?
Démontrer votre affirmation.

3. Soit $y \in G$ et $a \in G$ tels que $a \cdot y \cdot a^{-1}$ appartient au groupe engendré par y.
Montrer que pour tout $k \in \mathbb{N}$, $a \cdot y^k \cdot a^{-1}$ appartient au groupe engendré par y.

Partie 2 : le groupe des quaternions

On désigne par $SL_2(\mathbb{C})$ l'ensemble des matrices carrées 2×2 à coefficients dans le corps des nombres complexes $\mathbb{C}$ de déterminant égal à 1.

1. Déterminer G_1, G_2 (en précisant leurs lois) et une application f de G_1 dans G_2 tels que $SL_2(\mathbb{C})$ soit le noyau du morphisme de groupes $f : G_1 \to G_2$.
Que peut-on en déduire ?

Exceptionnellement ***dans cet exercice****, l'énoncé utilisera des lettres minuscules en gras (*$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}, \boldsymbol{h}$ *par exemple) pour désigner des* ***matrices****. La lettre “ i ” sert comme d'habitude à désigner un nombre complexe tel que* $i^2 = -1$.

On considère le sous-groupe multiplicatif $\mathcal{H}_8$ de $SL_2(\mathbb{C})$ engendré par les deux matrices $\boldsymbol{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\boldsymbol{b} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

On note $\boldsymbol{i}_2$ la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2. Déterminer les ordres des éléments $\boldsymbol{a}$ et $\boldsymbol{b}$.

3. On admet pour l'instant que $\mathcal{H}_8$ est fini. Que peut-on en déduire concernant son cardinal ?

4. Le groupe $\mathcal{H}_8$ est-il commutatif ? Les groupes $\mathcal{H}_8$ et $\mathbb{U}_8$ peuvent-ils être isomorphes ?

On admet pour gagner un peu de temps que $\mathcal{H}_8 = \{\pm \boldsymbol{i}_2, \pm \boldsymbol{a}, \pm \boldsymbol{b}, \pm \boldsymbol{ab}\}$.
(vérifier que son cardinal vérifie la condition de la question **3.**)

5. Déterminer les ordres des 6 éléments $-\boldsymbol{a}, -\boldsymbol{b}, \pm \boldsymbol{ab}, \pm \boldsymbol{i}_2$.

6. Montrer que les sous groupes de $\mathcal{H}_8$ sont :

$$\{\boldsymbol{a}, -\boldsymbol{i}_2, -\boldsymbol{a}, \boldsymbol{i}_2\}, \{\boldsymbol{b}, -\boldsymbol{i}_2, -\boldsymbol{b}, \boldsymbol{i}_2\}, \{\boldsymbol{ab}, -\boldsymbol{i}_2, -\boldsymbol{ab}, \boldsymbol{i}_2\}, \{-\boldsymbol{i}_2, \boldsymbol{i}_2\}, \{\boldsymbol{i}_2\} \text{ et } \mathcal{H}_8.$$

7. Vérifier que tout sous groupe de $\mathcal{H}_8$ **différent de** $\mathcal{H}_8$ est cyclique et en préciser un générateur.

8. Déterminer les sous groupes $\mathcal{H}$ de $\mathcal{H}_8$ tels que pour toute matrice $\boldsymbol{m}$ de $\mathcal{H}_8$, on ait $\boldsymbol{m} \cdot \mathcal{H} \cdot \boldsymbol{m}^{-1} = \mathcal{H}$.

On rappelle que $\boldsymbol{m} \cdot \mathcal{H} \cdot \boldsymbol{m}^{-1} = \{\boldsymbol{m} \cdot \boldsymbol{h} \cdot \boldsymbol{m}^{-1} | \boldsymbol{h} \in \mathcal{H}\}$.

Partie 3 : le corps des quaternions

À n'aborder QUE si tout ce qui précède a été traité

Dans cette partie, les lettres z et z' désignent des nombres complexes. Alors $\overline{z}$ désigne le conjugué de z.
On utilisera toujours les lettres minuscules $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ et $\boldsymbol{i}_2$ pour désigner des matrices.

On définit l'ensemble

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -z' \\ \overline{z'} & \overline{z} \end{pmatrix} | (z, z') \in \mathbb{C}^2 \right\}$$

1. Vérifier que $(\mathbb{H}, +, \cdot)$ est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$.

2. On note $\boldsymbol{i}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\boldsymbol{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\boldsymbol{b} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et $\boldsymbol{c} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ et $\boldsymbol{0}$= $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Montrer que toute matrice $\boldsymbol{q} \in \mathbb{H}$ s'écrit de manière unique comme combinaison linéaire **à coefficients réels** des matrices $\boldsymbol{i}_2$, $\boldsymbol{a}$, $\boldsymbol{b}$ et $\boldsymbol{c}$.

Soit $\boldsymbol{q} = x\boldsymbol{i}_2 + a\boldsymbol{a} + b\boldsymbol{b} + c\boldsymbol{c}$. On pose $\boldsymbol{q}^* = x\boldsymbol{i}_2 - a\boldsymbol{a} - b\boldsymbol{b} - c\boldsymbol{c}$.

3. Justifier rapidement que si $\boldsymbol{q} \in \mathbb{H}$, alors $\boldsymbol{q}^* \in \mathbb{H}$.

Pour gagner un peu de temps, on admet que si $\boldsymbol{q}_1$ et $\boldsymbol{q}_2$ sont dans $\mathbb{H}$, alors $(\boldsymbol{q}_1 \cdot \boldsymbol{q}_2)^* = \boldsymbol{q}_2^* \cdot \boldsymbol{q}_1^*$.

4. On note $\mathbb{H}^* = \mathbb{H} \setminus \{\boldsymbol{0}\}$. Déduire de ce qui précède que l'application

$$\begin{array}{rccc} N: & (\mathbb{H}^*, \cdot) & \to & (\mathbb{R}_+^*, \times) \\ & \mathbf{q} & \mapsto & \mathbf{q}\mathbf{q}^* \end{array}$$

est un morphisme de groupes.

5. Montrer que $(\mathbb{H}, +, \cdot)$ est un corps non commutatif.

II — Rapport et éléments de correction

Ce qui est indiqué en italique correspond au rapport de l'épreuve : cela indique les erreurs majoritairement commises à éviter ou faiblesses à corriger pour les prochains devoirs sous peine d'être lourdement sanctionné !

CONSEILS GÉNÉRAUX :
- *aucune abréviation (l.c.i., s.g., ...) n'est autorisée !!!*
- *pour l'apprentissage du cours : BIEN DISTINGUER les différentes notions (fonctions, éléments, produits, itérés, inverses, ...)*
- *pour la rédaction : BIEN CONTRÔLER que ce qui est écrit A UN SENS !*

1) Théorème de Lagrange dans un groupe commutatif

Dans ce type de "question de cours" (on peut en retrouver à l'écrit comme à l'oral), il convient de lire l'INTÉGRALITÉ du sujet pour s'imprégner de son esprit et éviter de répondre trop tôt à des questions, utiliser des résultats qui sont implicitement non admis ou utiliser des marteaux pilons pour écraser des mouches... Bref, ceux qui utilisent le résultat de la question 5. pour répondre à la question 1. sont bien HORS SUJET !

1. *Il faut ajouter "non nul" à l'énoncé.* L'ensemble $\{a^n | n \in \mathbb{N}^*\} \subset G$. Or G est fini. Donc il existe $N_1 < N_2$ dans $\mathbb{N}^*$ tels que $a^{N_1} = a_{N_2}$. En multipliant par a^{-N_1}, on obtient que $a^{N_2-N_1} = e$, donc l'ensemble des entiers naturels **non nuls** tels que $a^n = e$ n'est pas vide et minoré, donc admet un plus petit élément.

On ne peut pas utiliser le th de Lagrange pour cette question : le but de l'exercice est justement de démontrer ce théorème !

2. En faisant un division euclidienne : $n = n_0 \cdot q + r$ donc $a^n = a^{n_0 q + r} = a^r$ car $a^{n_0} = e$. Or $0 \leq r < n_0$. Par statut de n_0, on doit avoir $r = 0$ et n_0 divise donc n.

3. P est un produit d'éléments de G et G est un groupe (donc stable par produit).

4. *On peut très bien vérifier l'injectivité puis la surjectivité de f_a. MAIS pour l'injectivité , il faut revenir à la définition générale et faire attention de ne pas parler du noyau de f_a qui N'EST PAS un morphisme de groupes (par exemple $f_a(e) = a \neq e$ en général..*

On peut vérifier que l'application $f_{a^{-1}}$ est telle que $f_{a^{-1}} \circ f_a = f_a \circ f_{a^{-1}} = Id_G$, donc f_a est une bijection de G dans G. On peut aussi montrer que f_a est à la fois injective et surjective à la main ou même ne faire que l'un et utiliser un argument de cardinalité.

5. $\prod_{g \in G} f_a(g) = \prod_{g \in G} g$ d'après la question précédente.
D'autre part, comme G est commutatif, $\prod_{g \in G} f_a(g) = a^{Card(G)} \cdot \prod_{g \in G} g$. Comme l'élément $\prod_{g \in G} g$ est régulier dans G, on obtient que $a^{Card(G)} = e$. D'après la question **2.**, l'ordre de a divise $Card(G)$.

6. Iinitialiser k à 1 (pas à 0 car $a^0 = e$ et on risque de sortir de la boucle prématurément) puis créer une boucle conditionnelle `while` qui incrémente k de 1 et calcule a^k à l'aide de la relation de récurrence $\mathtt{a}^k$ =`Mult(`$\mathtt{a}^{k-1}$`,a)` jusqu'à ce que $\mathtt{a}^k$ soit égal à `e`.

Renvoyer alors la dernière valeur de k.

```
def ordre(a):
    k=1
    P = a
    while P!=e:
        P=Mult(P,a)
        k=k+1
    return(k)
```

On rencontre assez souvent l'erreur qui consiste à utiliser à chaque itération une formule équivalente à `a=Mult(a,a)`*, ce qui a pour effet de calculer successivement $a, a^2, a^4, a^8, \ldots$ à la place de $a, a^2, a^3, a^4, \ldots$*

2) Opérations ensemblistes sur les sous groupes

1. L'intersection de deux sous groupes est un sous groupe (cela reste vrai pour une intersection quelconque). La démonstration est dans le cours.

2. Le produit cartésien de deux groupes est un groupe pour la loi du produit. Démonstration dans le cours.

Erreur courante ici : le produit cartésien de deux sous groupes N'EST PAS un sous groupe !!! Le produit cartésien de H_1 et H_2 est un ensemble de COUPLES d'éléments de G, donc n'est pas inclus dans G !

3. Le complémentaire d'un sous groupe ne contient jamais le neutre et donc n'est jamais un sous groupe.

4. L'union dans $(\mathbb{R}^2, +)$ des sous groupes engendrés par $(1,0)$ et $(0,1)$ n'est pas un sous groupe car par exemple, $(1,1) = (1,0) + (0,1)$ n'est pas dans cet ensemble.

Le résultat est connu de la majorité, mais bizarrement, le contre exemple est trop souvent absent des copies ! Voilà des points trop facilement perdus !

5. a. Cette dernière hypothèse signifie que H_1 n'est pas inclus dans H_2.

Le produit $x \cdot y$ est dans $H_1 \cup H_2$ car $x \in H_2 \subset H_1 \cup H_2$ et $y \in H_1 \subset H_1 \cup H2$. Comme $H_1 \cup H_2$ est un sous groupe (stable par multiplication), le produit $x \cdot y$ est bien dans $H_1 \cup H_2$.

Donc $x \cdot y \in H_1$ ou bien $x \cdot y \in H_2$. Or, il est impossible que $x \cdot y \in H_2$ car sinon, $x^{-1} \cdot (x \cdot y) = y$ devrait appartenir à H_2 ce qui n'est pas. Finalement, $xy \in H_1$ et $x = (xy) \cdot y^{-1} \in H_1$.

b. On vient de démontrer que $H_2 \subset H_1$.

6. On vient de démontrer que si H_1 n'est pas inclus dans H_2, nécessairement H_2 est inclus dans H_1.

Donc pour que $H_1 \cup H_2$ soit un sous groupe, il est nécessaire que l'un des deux sous groupes soit inclus dans l'autre !

C'est clairement une condition suffisante : en effet, si $H_1 \subset H_2$, alors $H_1 \cup H_2 = H_2$ qui est un sous groupe et si $H_2 \subset H_1$, alors $H_1 \cup H_2 = H_1$ qui est un sous groupe...

7. Il suffit que l'un des sous groupes soit inclus dans l'autre : par exemple $H_1 = 2\mathbb{Z}$ et $H_2 = 2016\mathbb{Z}$.

3) Matrices triangulaires

1. L'ensemble G est inclus dans le groupe $(GL_3(\mathbb{R}), \times)$ (par exemple en utilisant que le déterminant d'une matrice triangulaire supérieure est égal au produit des termes diagonaux, donc ici non nul). Il suffit donc de montrer que cela en est un sous groupe. *Attention : $(M_3(\mathbb{R}), \times)$ N'EST PAS un groupe !*

— L'ensemble G n'est pas vide (contient par exemple la matrice I_3)

— G est stable par multiplication car le produit de deux matrices triangulaires supérieures est une matrice triangulaire supérieure dont les termes diagonaux sont les produits des termes diagonaux ($1 = 1 \times 1$).

— *Pour le symétrique, il ne suffit pas de montrer que tout élément de G est inversible : il faut aussi vérifier que son inverse est dans G : on doit donc faire quelques calculs !!!*

En résolvant un système de 3 équations à 3 inconnues, on trouve que

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \in G$$

Donc G est un sous groupe de $(GL_3(\mathbb{R}), \times)$, donc un groupe.

2. Soit l'ensemble $\mathbb{R}^2$ muni de la loi $(a_1, b_1) +_{\mathbb{R}^2} (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. C'est le produit cartésien de $(\mathbb{R}, +)$ par lui même donc un groupe d'après le cours.

3. On vérifie aisément que

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x'' & y'' \\ 0 & 1 & z'' \\ 0 & 0 & 1 \end{pmatrix}.$$

Donc pour $(A, B) \in G^2, f(AB) = f(A) + f(B)$.

4. Soient $(x, z) \in \mathbb{R}^2$. Alors en particulier, $f(\begin{pmatrix} 1 & x & 0 \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}) = (x, z)$ donc f est surjective et $Im(f) = \mathbb{R}^2$.

D'autre part, si $A = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$, $f(A) = (0,0)$ ssi $A = \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Donc $Ker(f) = \left\{ \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} |y \in \mathbb{R} \right\}$

4) Deux groupes non isomorphes

Par l'absurde, soit f un isomorphisme de $(\mathbb{Z},+)$ dans $(\mathbb{Q},+)$.
Soit $r = f(1)$. Remarquons que $r \neq 0$ car $Ker(f) = \{0\}$. Le rationnel $r/2$ admet un antécédent par f, disons $a \in \mathbb{Z}$. Remarquons encore que $a \neq 0$, cette fois car $f(0) = 0 \neq r/2$. On doit alors avoir $f(2a) = f(a+a) = f(a)+f(a) = r = f(1)$. Comme f est un isomorphisme donc bijectif, on a donc $2a = 1$ dans $\mathbb{Z}$, ce qui est absurde.

En modifiant très légèrement cette démonstration, on obtient même que le seul morphisme de $(\mathbb{Z},+)$ dans $(\mathbb{Q},+)$ est l'application nulle...

5) Les quaternions

Partie 1 : des résultats généraux utiles

1. Voir le cours.

2. *Erreur courante : l'égalité $x^4 = e$ N'IMPLIQUE PAS que $O(x) = 4$ mais plutôt que $O(x)$ DIVISE 4. Il faut donc ENSUITE vérifier que $O(x) \notin \{1,2\}$ pour conclure !*
Soit x tel que $x^2 = g$. Alors $x^4 = e$. L'ordre $O(x)$ de l'élément x est donc fini et divise 4. Or $O(x) \notin \{1,2\}$ car $x^2 = g \neq e$, donc $O(x) = 4$.

3. *Dans ce genre de question, une récurrence est exigée. On ne peut pas se contenter de dire que le résultat "se voit" bien ! Une minorité ne sait pas bien rédiger une récurrence (notamment l'énoncé de la propriété P_n à démontrer ou bien le rappel de l'hypothèse de récurrence dans l'hérédité).*
Par récurrence : soit $n \in \mathbb{N}$ et P_n la propriété : "$a \cdot y^n \cdot a^{-1}$ appartient au groupe engendré par y"
P_0 est vraie car $ay^0a^{-1} = aea^{-1} = e \in < y >$.
Soit $n \in \mathbb{N}$ tel que P_n soit vraie. Alors $a \cdot y^n \cdot a^{-1}$ appartient au groupe engendré par y. Or d'après l'énoncé, $aya^{-1} \in < y >$ également. Donc par stabilité par produit, $(ay^na^{-1}) \cdot (aya^{-1})$ appartient au groupe engendré par y et par associativité et en utilisant que $aa^{-1} = e$, on obtient que $a \cdot y^{n+1} \cdot a^{-1}$ appartient au groupe engendré par y.
Récurrence établie.

Partie 2 : le groupe des quaternions

On désigne par $SL_2(\mathbb{C})$ l'ensemble des matrices carrées 2×2 à coefficients dans le corps des nombres complexes $\mathbb{C}$ de déterminant égal à 1.

1. Posons $(G_1,\cdot) = (GL_3(\mathbb{C}),\cdot)$ et $(G_2,\cdot) = (\mathbb{C}^*,\cdot)$. Posons alors $f = det$. f est un morphisme de groupes car $det(AB) = det(A)det(B)$. $(SL_2(\mathbb{C}),\cdot)$ est alors le noyau de ce morphisme, donc un sous groupe de $(GL_3(\mathbb{C}),\cdot)$ donc un groupe.

2. On trouve $\mathbf{a}^2 = -\mathbf{i}_2$ donc $\mathbf{a}$ est d'ordre 4 d'après la question **2**. de la partie 1. Idem pour $\mathbf{b}$.

3. Par le théorème de Lagrange, le cardinal de $\mathcal{H}_8$ doit être un multiple de 4.
Bizarement, on retrouve plusieurs fois l'affirmation fausse : le cardinal de $\mathcal{H}_8$ divise le cardinal de $SL_2(\mathbb{C})$. La confusion est double : on a ici affaire à un élément de $\mathcal{H}_8$ qui donc donne une information sur l'ordre de $\mathcal{H}_8$. Rien à voir avec $SL_2(\mathbb{C})$ qui lui est infini...

4. On vérifie que $\mathbf{ab} \neq \mathbf{ba}$ donc $\mathcal{H}_8$ n'est pas commutatif. Il ne peut donc pas être isomorphe à $\mathbb{U}_8$ qui lui est cyclique DONC commutatif (laissé en exercice...).
Coin de la culture : à isomorphisme près, il n'y a que 5 groupes de cardinal 8 dont deux non commutatifs.

5. Pour les mêmes raisons qu'à la question 2., les ordres de $-\boldsymbol{a}, -\boldsymbol{b}, \pm\boldsymbol{ab}$ sont tous égaux à 4.
L'ordre de $-\mathbf{i}_2$ est égal à 2 et celui de $\mathbf{i}_2$ est égal à 1.

6. Le sous groupes $G_a = \{\boldsymbol{a}, -\boldsymbol{i}_2, -\boldsymbol{a}, \boldsymbol{i}_2\}$ est égal au sous groupe cyclique engendré par $\mathbf{a}$.
Le sous groupe $G_b = \{\boldsymbol{b}, -\boldsymbol{i}_2, -\boldsymbol{b}, \boldsymbol{i}_2\}$ est égal au sous groupe cyclique engendré par $\mathbf{b}$
Le sous groupe $G_{ab} = \{\boldsymbol{ab}, -\boldsymbol{i}_2, -\boldsymbol{ab}, \boldsymbol{i}_2\}$ est égal au sous groupe cyclique engendré par $\mathbf{ab}$.
Le sous groupe $G_{-1} = \{-\boldsymbol{i}_2, \boldsymbol{i}_2\}$ est égal au sous groupe cyclique engendré par $-\mathbf{i}_2$.
Les sous groupes $\{\boldsymbol{i}_2\}$ *et* $\mathcal{H}_8$ sont les sous groupes triviaux.
Il ne peut pas y en a pas d'autres : en effet , par théorème de Lagrange, tout sous groupe doit avoir un cardinal divisant 8.
Le seul sous groupe de cardinal 1 est le groupe trivial $\{\boldsymbol{i}_2\}$.
Si un sous groupe est de cardinal 2, il ne peut pas contenir d'éléments d'ordre strictement supérieur à 2, donc est forcément égal à G_{-1}.
Enfin, il est facile de vérifier que $< \boldsymbol{a}, \boldsymbol{b} > = < \boldsymbol{a}, \boldsymbol{ab} > = < \boldsymbol{b}, \boldsymbol{ab} > = \mathcal{H}_8$. Donc les seuls groupes d'ordres 4 sont ceux cités plus haut.

7. Voir question précédente.

8. De tels sous groupes sont dits **normaux**. Pour éviter de faire trop de calculs fastidieux, on utilise la question **3.** de la partie 1 : pour un groupe cyclique $< g >$, il suffit de vérifier que $\forall m \in \mathcal{H}_8, m \cdot g \cdot m^{-1} \in < g >$.
On vérifie alors que c'est vrai pour $g = \mathbf{a}, \mathbf{b}, \mathbf{ab}, -\mathbf{i}_2$ ou $\mathbf{i}_2$. Donc TOUS les sous groupes stricts de $\mathcal{H}_8$ sont **normaux**.
Enfin, $\mathcal{H}_8$ est **normal** (tout groupe est **normal** dans lui même).