DEVOIR SURVEILLÉ n° 0 (2H)

Jeudi 12 septembre 2019

I — Questions de cours

1. Donner la définition d'un groupe monogène.

Un groupe $(G, \cdot)$ est monogène ssi il existe $g \in G$ tel que $< g >= G$.

On peut mentionner qu'un tel g est appelé générateur de G et qu'il n'est pas nécessairement unique à avoir ce statut.

Donner la définition d'un groupe cyclique.

Un groupe cyclique est un groupe monogène de cardinal fini.

Donner un exemple d'un groupe non monogène.

$(\mathbb{Z}^2, +)$ n'est pas monogène (voir plus loin).

Donner l'exemple d'un groupe monogène non cyclique.

$(\mathbb{Z}, +)$ est monogène en gendré par 1. Mais il est infini, donc n'est pas cyclique.

2. Énoncer le théorème de structure des groupes monogènes.

Soit $(G, \cdot)$ est un groupe monogène.

Si G est fini, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Si G est infini, il est isomorphe à $\mathbb{Z}$.

3. Énoncer le théorème des restes chinois.

Si n, p sont deux entiers premiers entre eux, alors $\mathbb{Z}/np\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sont isomorphes. L'application $\phi : x \bmod np \mapsto (x \bmod n, x \bmod p)$ est par exemple un isomorphisme entre ces deux groupes.

4. Énoncer puis démontrer le théorème de Lagrange.

Dans un groupe fini G, l'ordre de tout élément $g \in G$ divise le cardinal du groupe G. C'est à dire : $\forall a \in G, a^{Card(G)} = e_G$.

Dans le cas où G est commutatif, on pose $P = \prod_{g \in G} g$. Soit $a \in G$. L'application $\phi_a : g \mapsto ag$ est bijective de bijection réciproque $\phi_{a^{-1}}$. C'est donc une permutation de G. Donc $P' = \prod_{g \in G} ag = P$. Par ailleurs, $P' = a^{Card(G)}$ car G est commutatif. En multipliant par P^{-1}, on obtient $a^{Card(G)} = e_G$.

5. Démontrer que les sous groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

Les $(n\mathbb{Z}, +)$ sont des sous groupes de $(\mathbb{Z}, +)$ par caractérisation des sous groupes.

Réciproquement, soit H est un sous groupe de $(\mathbb{Z},+)$. Si $H=\{0\}$, alors $H=0\mathbb{Z}$. Sinon, $H\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément noté n.

D'une part, $n\mathbb{Z}\subset H$ car H est un sg.

D'autre part, si $h\in H$, par th. de division euclidienne, il existe $(q,r)\in\mathbb{Z}^2$ tel que $h=qn+r$ et $0\leqslant r<n$.

Alors $r=n-qn\in H\cap\mathbb{N}$. Comme $r<n$, $r=0$ par statut de n. Donc $h\in n\mathbb{Z}$ et $H=n\mathbb{Z}$.

6. Quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$? Justifier qu'ils sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$.

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les classes d'équivalence $x\mathrm{mod}n$ avec x et n premiers entre eux.

Si x et n sont premiers entre eux, par relation de Bézout, il existe u,v entiers tels que $xu+vn=1$, donc $(x\ mod\ n)(u\ mod\ n)=(1\ mod\ n)$, donc $x\ modn$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Son inverse est $u\ mod\ n$.

7. Donner l'exemple d'un groupe non commutatif de cardinal 6.

S_3 le groupe de permutations de trois éléments convient.

II — Questions d'applications directes du cours

1. Montrer que si $(G,\cdot)$ est un groupe tel que $\phi:x\mapsto x^{-1}$ est un morphisme de groupes, alors G est commutatif.

On doit montrer que $\forall(x,y)\in G^2, xy=yx$.

Soient x,y dans G. Alors $\phi(xy)=(xy)^{-1}$. Comme ϕ est un morphisme, $\phi(xy)=\phi(x)\phi(y)=x^{-1}y^{-1}$.

Alors $(xy)^{-1}=x^{-1}y^{-1}$. En passant cette égalité à l'inverse, on obtient $xy=(x^{-1}y^{-1})^{-1}=(y^{-1})^{-1}(x^{-1})^{-1}=yx$.

Remarque : on pouvait aussi partir de $\phi(x^{-1}y^{-1})$ et obtenir directement le résultat.

2. Déterminer les solutions du système :

$$\begin{cases} x\equiv 2[3] \\ x\equiv 5[7] \\ 2x\equiv -1[11] \end{cases}.$$

On pourra résoudre le système $\begin{cases} x\equiv 2[3] \\ x\equiv 5[7] \end{cases}$ puis remarquer que 2 et 11 sont premiers entre eux.

D'après le théorème des restes chinois, comme 3 et 7 sont premiers entre eux, le système $\begin{cases} x\equiv 2[3] \\ x\equiv 5[7] \end{cases}$ est équivalent à une équation $x\equiv x_0[21]$ où x_0 est une solution particulière. Par exemple, $x_0=5$ convient.

Notre problème est donc de résoudre

$$\begin{cases} x\equiv 5[21] \\ 2x\equiv -1[11] \end{cases}.$$

Dans la seconde équation, 2 et 11 sont premiers entre eux : donc la classe de 2 est inversible modulo 11. Son inverse est d'ailleurs la classe de 6 car $2\times 6=12=1+11$. Donc $2x\equiv -1[11]$ est équivalente à $x\equiv -6[11]$.

Notre problème est donc équivalent à

$$\begin{cases} x \equiv 5[21] \\ x \equiv -6[11] \equiv 5[11] \end{cases}.$$

Comme 21 et 11 sont premiers entre eux, on termine la résolution de ce sysètme par théorème des restes chinois et on trouve $x \equiv 5[231]$.

3. Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}^{+*}, \cdot)$.

Que vaut $f(0)$?

0 est le neutre de $(\mathbb{Q}, +)$*. Par un morphisme, il est envoyé sur le neutre de* $(\mathbb{Q}^{+*}, \cdot)$ *qui est égal à 1. Donc* $f(0) = 1$.

Calculer $f(n)$ en fonction de $f(1)$ pour tout entier $n \in \mathbb{Z}$.

$f(n) = f(1 + 1 + \cdots + 1) = f(n \cdot 1) = (f(1))^n$ *(attention à ne pas confondre les structures multiplicatives et additives)*

Calculer $f(1/n)$ en fonction de $f(1)$ pour tout entier $n \in \mathbb{N}^*$.

Par un raisonnement similaire, comme $f(n \cdot 1/n) = f(1)$*, on obtient* $f(1/n)^n = f(1)$ *comme* f *est un morphisme de groupes. Donc*

$$f(1/n) = (f(1))^{1/n} = \sqrt[n]{f(1)}.$$

Montrer que $(\mathbb{Q}, +)$ et $(\mathbb{Q}^{+*}, \cdot)$ ne sont pas isomorphes.

Si par l'absurde, il existe f *isomorphisme entre* $(\mathbb{Q}, +)$ *et* $(\mathbb{Q}^{+*}, \cdot)$*, comme* f *est surjective, il exsite* $a \in \mathbb{Q}$ *tel que* $f(a) = 2$*. Alors* $f(a/2) = \sqrt{f(a)} = \sqrt{2}$*. Or* $\sqrt{2} \notin \mathbb{Q}^{+*}$*. Donc* $a/2$ *ne peut pas avoir d'image : une telle fonction* f *ne peut pas être définie.*

4. Montrer que si n et p sont des entiers premiers entre eux et qu'un élément z d'un groupe G vérifie $z^n = z^p = e$ où e est le neutre de G, alors $z = e$.

Si n *et* p *sont premiers entre eux, il existe* u, v *entiers tels que* $nu + vp = 1$*. Alors* $z = z^{nu+vp} = (z^n)^u \cdot (z^p)^p = e \cdot e = e$.

Montrer que si n et p sont premiers entre eux, l'application

$$\varphi : \begin{cases} \mathbb{U}_n \times \mathbb{U}_p & \to & \mathbb{U}_{np} \\ (z_1, z_2) & \mapsto & z_1 z_2 \end{cases}$$

est un isomorphisme de groupes.

Répondons à la question posée...

- *La fonction* φ *est un morphisme de groupes : en effet, soit* (z_1, z_2) *et* (z_1', z_2') *dans* $n \times p$*.* $\varphi((z_1, z_2) \times (z_1', z_2')) = \varphi((z_1 z_1', z_2 z_2') = (z_1 z_1')(z_2 z_2') = (z_1 z_2)(z_1' z_2') = \varphi((z_1, z_2)) \cdot \varphi((z_1', z_2'))$.
- φ *est injective car* $Ker(\varphi) = \{(z_1, z_2) | z_1 z_2 = 1\}$*. Si* $z_1 z_2 = 1$*, alors* $(z_1 z_2)^n = z_1^n z_2^n = 1 \cdot z_2^n = 1$*. En particulier,* $z_2^n = 1$*. Or* $z_2^p = 1$ *car* $z_2 \in p$*. D'après ce qui précède,* $z_2 = 1$*. De même,* $z_1 = 1$*. Finalement,* $Ker(\varphi) = \{(1, 1)\}$.
- *Comme* $Card(n \times p) = np = Card(np)$*, l'injectivité de* φ *est équivalente à la surjectivité de* φ.

Finalement, φ *est bien un isomorphisme...*

5. 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.

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

Initialiser 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* `a`^{k} =`Mult(a`$^{k-1}$`,a)` *jusqu'à ce que* `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 $a, a^2, a^3, a^4, \ldots$

III — Problème : groupe spécial linéaire et quaternions

Les deux parties de ce problème sont totalement indépendantes.
*Exceptionnellement **dans ce problème**, l'énoncé utilisera des lettres minuscules en gras ($\mathbf{a}, \mathbf{b}, \mathbf{m}, \mathbf{h}$ par exemple) pour désigner des **matrices**. La lettre " i " sert comme d'habitude à désigner un nombre complexe tel que $i^2 = -1$.*

Partie 1 : le groupe spécial linéaire et groupe quotient $GL_n(\mathbb{C})/SL_n(\mathbb{C})$.

On note $G = GL_n(\mathbb{C})$ et $H = SL_n(\mathbb{C})$ l'ensemble des matrices à coefficients complexes et de déterminant égal à 1.

1. Montrer que H est un groupe en justifiant que H est le noyau d'un morphisme de groupes.
H est le noyau du morphisme $\det : (\mathcal{GL}_n(\mathbb{C}), \times) \to (\mathbb{C}^*, \times)$.

2. Montrer que $\forall \mathbf{a} \in G, \forall \mathbf{h} \in H, \mathbf{aha}^{-1} \in H$.
Les matrices sont inversibles et $det(aha^{-1}) = det(a)det(h)det(a^{-1}) = det(h) = 1$ car $h \in H$.

3. Pour $\mathbf{a}, \mathbf{b} \in G$, on pose la relation binaire :

$$\mathbf{a}\mathcal{R}_{\mathcal{H}}\mathbf{b} \Leftrightarrow \mathbf{ab}^{-1} \in H.$$

Montrer que $\mathcal{R}_H$ est une relation d'équivalence.
Soient $a, b, c \in G^3$:

- *$a\mathcal{R}a$ car $aa^{-1} = I_n \in H$.*
- *si $ab^{-1} \in H$, alors $(ab^{-1})^{-1} = ba^{-1} \in H$ car H est un sous groupe stable par inverse.*
- *si $ab^{-1} \in H$ et $bc^{-1} \in H$, alors $ab^{-1}bc^{-1} = ac^{-1} \in H$ car H est un sous groupe stable apr produit.*

4. On note G/H l'ensemble des classes d'équivalence. Montrer qu'on peut munir G/H d'une structure de groupe héritée de celle de G en posant

$$\forall\ (\overline{\mathbf{a}},\ \overline{\mathbf{b}}) \in (G/H)^2, \overline{\mathbf{a}} \times \overline{\mathbf{b}} := \overline{\mathbf{ab}}.$$

Il suffit de montrer que la définition de la loi $\times$ ne dépend pas du choix des représentants des classes $\overline{\boldsymbol{a}}$ et $\overline{\boldsymbol{b}}$.

Soient alors a et a', b et b' tels que $\overline{\boldsymbol{a}} = \overline{\boldsymbol{a'}}$ et $\overline{\boldsymbol{b}} = \overline{\boldsymbol{b'}}$.

Vérifions que $\overline{\boldsymbol{ab}} = \overline{\boldsymbol{a'b'}}$.

En effet, $\boldsymbol{ab} \cdot (\boldsymbol{a'b'})^{-1} = \boldsymbol{abb'^{-1}a'^{-1}} = \boldsymbol{aha'^{-1}}$ pour un $h \in H$. On a vu que $\boldsymbol{aha}^{-1} = h' \in H$. Donc $\boldsymbol{aha'^{-1}} = \boldsymbol{aha}^{-1}\boldsymbol{aa'^{-1}} = h'aa'^{-1} = h'h''$ où $h'' \in H$.

Finalement, $\boldsymbol{ab} \cdot (\boldsymbol{a'b'})^{-1} \in H$ donc la classe d'équivalence de $\boldsymbol{ab}$ est la même que celle de $\boldsymbol{a'b'}$.

5. Montrer que l'application déterminant $\det : (G/H, \times) \to (\mathbb{C}^*, \times)$ est une application définie de manière cohérente ($det(\overline{\mathbf{a}})$ ne dépend pas du représentant de la classe $\overline{\mathbf{a}}$).

Plus facile que la question précédente. Il s'agit de vérifier que si a et a' sont dans la même classe, alors $det(a) = det(a')$. C'est presque évident car si a et a' sont dans la même classe, il existe $h \in H$ tel que $a' = ah$ et $det(a') = det(ah) = det(a)det(h) = det(a)$ car $det(h) = 1$.

6. Montrer que $\det : (G/H, \times) \to (\mathbb{C}^*, \times)$ est un isomorphisme de groupes.

Soient $\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}} \in G/H$. D'après ce qui précède, $det(\overline{\boldsymbol{ab}}) = det(\boldsymbol{ab}) = det(\boldsymbol{a})det(\boldsymbol{b}) = det(\overline{\boldsymbol{a}})det(\overline{\boldsymbol{b}})$.

Partie 2 : le groupe des quaternions

1. Soit $(G, \cdot)$ un groupe multiplicatif. Soit X une partie non vide de G.
On note $< X >$ le sous groupe de G engendré par X.

a. On note $W = \{w \in G \mid \exists n \in \mathbb{N}, \exists (x_1, \dots x_n) \in X^n, w = x_1x_2 \dots x_n\}$.
Montrer que W est un sous groupe de G contenant X.

Il y a un pb dans l'énoncé : il faudrait lire $W = \{w \in G \mid \exists n \in \mathbb{N}, \exists (x_1, \dots x_n) \in (X \cup X^{-1})^n, w = x_1x_2 \dots x_n\}$

Dès lors, W n'est pas vide car X n'est pas vide et si $x \in X$, alors $e = x \cdot x^{-1} \in W$.

Si $w \in W$, on peut écrire $w = x_1x_2 \dots x_n$ où $(x_1, \dots x_n) \in (X \cup X^{-1})^n$. Alors $w^{-1} = x_n^{-1} \dots x_2^{-1}x_1^{-1} \in W$ car si $x_i \in X \cup X^{-1}$, $x_i^{-1} \in X \cup X^{-1}$ également.

b. En déduire que $< X > \subset W$.

$< X >$ est le plus petit sous groupe contenant X. Comme W contient X, il contient aussi $< X >$.

c. Montrer que $< X > = W$.

Il suffit de montrer que $< X >$ contient W. Soit $w \in W$, $w = x_1x_2 \dots x_n$. Comme $x_i \in X \cup X^{-1}$, $x_i \in < X >$. Par stabilité par produit, $w \in X$.

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.

On considère 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 $\mathcal{H}_8 = < \mathbf{a}, \mathbf{b} >$ le sous groupe engendré par $\mathbf{a}$ et $\mathbf{b}$.

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. Déterminer tous les éléments de $\mathcal{H}_8$. Vérifier que $Card(\mathcal{H}_8) = 8$.

4. Dresser la table de multiplication du groupe $\mathcal{H}_8$. Ce groupe est-il commutatif ? Les groupes $\mathcal{H}_8$ et $\mathbb{U}_8$ sont-ils isomorphes ?

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 :

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

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

IV — 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 $0 \leqslant r < n_0$. 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 `a`^{k} =`Mult(a`$^{k-1}$`,a)` jusqu'à ce que `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.

Bizaremment, 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).