Université Claude Bernard - Lyon 1 Semestre d'automne 2025-2026

L3 Math. Gén. : Groupes 05 novembre 2025

Correction de l'examen partiel (durée : 1h30)

Exercice 1 (Groupe de Heisenberg)**.** Soit $* : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ l'opération binaire définie pour tout $(a, b, c), (a', b', c') \in \mathbb{R}^3$ par :

$$(a, b, c) * (a', b', c') = (a + a', b + b', c + ab' + c'),$$

On admet pour cet exercice que $(\mathbb{R}^3, *)$ est un groupe.

1. Soit
$$H_3 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$
Montrer que H_3 est un sous-groupe de $GL_3(\mathbb{R})$ muni de la multiplication matricielle.
2. Montrer que H_3 muni de la multiplication matricielle est isomorphe à $(\mathbb{R}^3, *)$.

Correction 1. On admet que $(\mathbb{R}^3, *)$ est un groupe.

1. On remarque que pour tout $M \in H_3$ on a $\det(M) = 1$. Donc $H_3 \subseteq GL_3(\mathbb{R})$.
De plus $I_2 \in H_3$ donc $H_3 \neq \emptyset$.
Montrons que H_3 est clos par multiplication. Pour tout $a, b, c, a', b', c' \in \mathbb{R}^3$:
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & c + ab' + c' \\ 0 & 1 & b + b' \\ 0 & 0 & 1 \end{pmatrix} \in H_3$$
Montrons que pour tout $A \in H_3$ on a $A^{-1} \in H_3$.
Méthode 1 Soit $A \in H_3$. Comme $\det(A) = 1$ on a $A^{-1} = {}^t\mathrm{Com}(A)$. Or
$${}^t\mathrm{Com}(A) = \begin{pmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$
Comme $-a, -b, ab - c \in \mathbb{R}$ on a donc ${}^t\mathrm{Com}(A) \in H_3$, c'est-à-dire $A^{-1} \in H_3$.
Méthode 2 On pouvait aussi montrer que
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a - a & c - ab + ab - c \\ 0 & 1 & b - b \\ 0 & 0 & 1 \end{pmatrix} = I_3$$
Comme on est dans $GL_3(\mathbb{R})$, si une matrice admet un inverse à gauche c'est aussi un inverse à droite, donc $A^{-1} = \begin{pmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$ et $A^{-1} \in H_3$.
Donc H_3 est un sous-groupe de $GL_3(\mathbb{R})$.

2. Soit $f : H_3 \to \mathbb{R}^3$ telle que, pour tout $a, b, c \in \mathbb{R}$

$$f\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} = (a, b, c).$$

Montrons que f est un isomorphisme de $(H_3, \cdot)$ vers $(\mathbb{R}^3, *)$. Montrons d'abord que c'est un morphisme. Soient $a, b, c, a', b', c' \in \mathbb{R}^3$, on a

$$\begin{aligned} f\left(\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & a' & c'\\ 0 & 1 & b'\\ 0 & 0 & 1\end{pmatrix}\right) &= f\begin{pmatrix}1 & a+a' & c+ab'+c'\\ 0 & 1 & b+b'\\ 0 & 0 & 1\end{pmatrix},\\ &= (a+a', b+b', c+ab'+c'),\\ &= (a, b, c) * (a', b', c'),\\ &= f\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} * f\begin{pmatrix}1 & a' & c'\\ 0 & 1 & b'\\ 0 & 0 & 1\end{pmatrix}. \end{aligned}$$

Donc f est un morphisme de groupes. Montrons que f est bijectif. Pour tout $(a, b, c) \in \mathbb{R}^3$

$$f\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} = (a, b, c),$$

et f est donc surjectif. Déterminons maintenant $\ker(f)$. Soient $a, b, c \in \mathbb{R}$,

$$\begin{aligned} f\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} = (0,0,0) &\Rightarrow (a, b, c) = (0, 0, 0), \text{ (par définition de } f)\\ &\Rightarrow \begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = I_3. \end{aligned}$$

d'où $\ker(f) = \{I_3\}$ et f est donc injectif.
Donc f est un isomorphisme et ainsi $(H_3, \cdot)$ est isomorphe à $(\mathbb{R}^3, *)$.

Exercice 2 (Conjugaison)**.** *Les question 1 et 2 peuvent se traiter indépendamment*
Soit G un groupe.

1. Pour tout $A \subseteq G$ on note $C_G(A) := \{g \in G \ : \ \forall a \in A, \ gag^{-1} = a\}$ le centralisateur de A dans G. Soient $A, A' \subseteq G$.
   (a) Montrer que si $A \subseteq A'$ alors $C_G(A') \subseteq C_G(A)$.
   (b) Montrer que : $A \subseteq C_G(A')$ si et seulement si $A' \subseteq C_G(A)$
2. Soit $H \leq G$ un sous-groupe. Montrer que si le produit de deux classes à gauche modulo H est une classe à gauche modulo H, alors H est distingué dans G.

Correction 2. 1. Supposons $A \subseteq A'$. Soit $g \in C_g(A')$ et montrons que $g \in C_G(A)$.
Comme $g \in C_G(A')$, on a $gag^{-1} = a$ pour tout $a \in A'$. Comme $A \subseteq A'$, ceci implique en

particulier que $gag^{-1} = a$ pour tout $a \in A$, c'est-à-dire $g \in C_G(A)$.
Ainsi $C_G(A') \subseteq C_G(A)$.

2. *Pour aider à la compréhension, on propose ici une rédaction détaillée. Les lignes en gris n'étaient pas indispensables.*

$$\begin{aligned} A \subseteq C_G(A') &\Leftrightarrow \forall a \in A, a \in C_G(A'), \\ &\Leftrightarrow \forall a \in A, \forall b \in A'\ aba^{-1} = b, \text{(Par définition de } C_G(A')) \\ &\Leftrightarrow \forall b \in A', \forall a \in A,\ aba^{-1} = b, \text{(inversion de l'ordre des quantificateurs)} \\ &\Leftrightarrow \forall b \in A', \forall a \in A,\ a = bab^{-1}, \text{ (multiplication à droite par } ab^{-1}) \\ &\Leftrightarrow \forall b \in A', b \in C_G(A), \text{(Par définition de } C_G(A)) \\ &\Leftrightarrow A' \subseteq C_G(A). \end{aligned}$$

3. Soit $g \in G$. Le produit de deux classes à gauche modulo H étant une classe à gauche modulo H, il existe donc $x \in G$ tel que $(gH)(g^{-1}H) = xH$.
Montrons que $xH = H$. Pour cela, montrons que $e_G \in xH$.
Comme $e_G \in H$ on a $ge_G \in gH$ et $g^{-1}e_G \in g^{-1}H$. Ainsi

$$ge_Gg^{-1}e_G \in (gH)(g^{-1}H) = xH.$$

Mais $ge_Gg^{-1}e_G = e_G$. Donc $e_G \in xH$, et ainsi $e_GH = H \subseteq xH$ d'où $H = xH$ (deux classes à gauche sont égales ou disjointes). Ainsi $gHg^{-1}H = H$ et donc $gHg^{-1} \subseteq H$. Ceci étant vrai pour tout $g \in G$, on a donc montré que H est distingué dans G.

Exercice 3. Soit G un groupe fini de cardinal n et soit $m \in \mathbb{Z}$ tel que $\text{pgcd}(m, n) = 1$. Montrer que pour tout $a \in G$, l'équation $x^m = a$ admet une unique solution.

Correction 3. On propose deux rédactions.
Méthode 1 Comme $\text{pgcd}(m, n) = 1$ le théorème de Bézout implique qu'il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Ainsi, pour tout $a \in G$, on a

$$a^{um+vn} = a^1 = a.$$

Mais $a^{um+vn} = (a^u)^m(a^v)^n$. Or $(a^v)^n = e_G$ car $n = |G|$ (Lagrange). Donc

$$a = a^{um+vn} = (a^u)^m.$$

Ainsi $x = a^u$ est une solution de l'équation. Montrons maintenant l'unicité : soient $x, y \in G$ tels que $x^m = a = y^m$. Alors $(xy^{-1})^m = e_G$ et donc $\text{ord}(xy^{-1})$ divise m. Mais (Lagrange) $\text{ord}(xy^{-1})$ divise $|G| = n$. Ainsi $\text{ord}(xy^{-1})$ est un diviseur commun à m et n. Comme $\text{pgcd}(m, n) = 1$, on a ainsi $\text{ord}(xy^{-1}) = 1$, c'est-à-dire $xy^{-1} = e_G$. D'où $x = y$. Ce qui prouve l'unicité.
Méthode 2 Soit $\varphi : x \in G \mapsto x^m \in G$. Montrons que φ est bijective. Comme $\text{pgcd}(m, n) = 1$ le théorème de Bézout implique qu'il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Alors pour tout $a \in G$

$$a = a^1 = a^{um+vn} = (a^u)^m(a^v)^n = (a^u)^m.$$

Ainsi $\varphi(a^u) = a$. D'où la surjectivité de φ. De plus comme φ est surjective de G vers G et que $|G| < +\infty$, φ est nécessairement injective. La bijectivité de φ donne que pour tout $a \in G$ il existe un unique $x \in G$ tel que $a = x^m$.

Exercice 4 (Groupe symétrique)**.** *Les questions (1), (2), (3) et (4) peuvent se traiter indépendamment.*

(1) Soit G un groupe et H un sous-groupe de G d'indice 2. Montrer que pour tout $g \in G$, $g^2 \in H$.

(2) On se place dans S_9. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 8 & 6 & 2 & 9 & 4 & 7 \end{pmatrix}$.

(a) Décomposer σ en produit de cycles à supports disjoints et donner sa signature.

(b) Écrire σ^{-1} comme produit de cycles à supports disjoints.

(c) Déterminer $(12)\sigma(12)^{-1}$ et l'écrire comme produit de cycles à supports disjoints.

(3) Ici on se place dans S_n avec $n \geq 3$ et on rappelle que A_n est le noyau du morphisme signature $\varepsilon : S_n \to \{1, -1\}$.

(a) Justifier que tout 3-cycle est un carré.

(b) En utilisant les questions (1) et (3.a), montrer que A_4 n'admet pas de sous-groupes d'ordre 6.

(4) On se place à nouveau dans S_n avec $n \geq 3$.
Soit φ un automorphisme du groupe S_n tel que φ envoie une transposition sur une transposition. Pour $i = 2, \ldots, n$, on note $\tau_i = (1\ i)$.

(a) Soient τ et σ deux transpositions. Montrer qu'elles commutent si et seulement si leur support est disjoint. En déduire qu'il existe $a_1, a_2, a_3 \in \{1, \ldots, n\}$ distincts deux à deux tels que $\varphi(\tau_2) = (a_1\ a_2)$ et $\varphi(\tau_3) = (a_1\ a_3)$.

(b) En considérant à nouveau les supports et leurs intersections, montrer que pour tout $i \geq 4$, il existe $a_i \in \{1, \ldots, n\} \setminus \{a_1, a_2, a_3\}$ tel que $\varphi(\tau_i) = (a_1\ a_i)$.

(c) Justifier que l'application $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ qui envoie i sur a_i est un élément de S_n.

(d) Montrer que φ et l'application $\tau \mapsto \sigma \circ \tau \circ \sigma^{-1}$ coïncident. *On pourra montrer qu'elles coïncident sur les transpositions τ_i et utiliser un résultat vu en TD.*

Correction 4.

1. Soit $g \in G$. Si $g \in H$ alors g^2 aussi. Sinon, par hypothèse sur l'indice de H, on aura $G = H \sqcup gH$. Ainsi $g^2 \in H$ ou $g^2 \in gH$ et si $g^2 \in gH$ alors $g \in H$ ce qui est absurde.

2. (a) $\sigma = (13)(256)(48)(79)$ et $\varepsilon(\sigma) = (-1)^3(-1)^2 = -1$.

   (b) $\sigma^{-1} = (13)(652)(48)(79)$.

   (c) $(12)\sigma(12) = (48)(79)(12)(13)(256)(12) = (48)(79)(156)(23)$.

3. (a) Soit τ un 3-cycle. Alors $\tau^3 = \mathrm{Id}$ d'où $\tau = \tau^4 = (\tau^2)^2$.

(b) Supposons par l'absurde que A_4 admette un sous-groupe H d'ordre 6. Notons que $|A_4| = |S_4|/2 = 12$ et donc $[A_4 : H] = 2$. Par les questions (1) et (3.a), tous les 3-cycles sont dans H. Ainsi les six 3-cycles suivants sont dans H : (123), (132), (124), (142), (234), (243) en plus de l'identité ce qui fait que $|H| \geq 7$ ce qui est absurde.

4. (a) Notons $(a_1\ a_2) = \varphi(\tau_2) = \varphi((12))$ et $(a_3\ a_4) = \varphi(\tau_3) = \varphi((13))$ (ce sont des transpositions par hypothèse). Puisque τ_2 et τ_3 ne commutent pas, il en est de même pour $\varphi(\tau_2)$ et $\varphi(\tau_3)$ donc leur support ne sont pas disjoints. Ainsi $a_3 \in \{a_1, a_2\}$ ou $a_4 \in \{a_1, a_2\}$. Par symétrie, on peut suppose que $a_4 \in \{a_1, a_2\}$ et quitte à réindexer, on peut supposer que $a_4 = a_1$ ce qui donne $\varphi(\tau_1) = (a_1\ a_2)$ et $\varphi(\tau_2) = (a_1\ a_3)$.

(b) On a : $\tau_i = (1i)$, $\tau_2 = (12)$ et $\tau_3 = (13)$. Donc $\varphi(\tau_i)$ a son support non-disjoint de celui de $\varphi(\tau_2) = (a_1a_2)$ et de $\varphi(\tau_3) = (a_1a_3)$. On a alors deux cas possibles : $\varphi(\tau_i) = (a_1a_i)$ avec $a_i \notin \{a_1, a_2, a_3\}$ (n'oublions pas que φ est bijective) ou bien $\varphi(\tau_i) = (a_2a_3)$. Supposons par l'absurde que $\varphi(\tau_i) = (a_2a_3)$. On a $(12)(1i)(12) = (2i)$. En appliquant φ, on obtient $(a_1a_2)(a_2a_3)(a_1a_2) = \varphi((2i))$, i.e. $(a_1a_3) = \varphi((2i))$ i.e. $\varphi((13)) = \varphi((2i))$ d'où $(13) = (2i)$. Absurde.

(c) Les a_i sont distincts deux à deux car sinon on aurait $(a_1a_i) = (a_1a_j)$ avec $i \neq j$ puis via φ^{-1}, $\tau_i = \tau_j$. Ainsi l'application qui envoie i sur a_i est injective et donc bijective (pour des questions de cardinal).

(d) Soient $i, j \in \{1, \ldots, n\}$. Alors, d'une part, $\varphi(\tau_i) = (a_1a_i)$. D'autre part,

$$\sigma \circ \tau_i \circ \sigma^{-1}(a_j) = \sigma \circ \tau_i(j) = \begin{cases} a_j \text{ si } j \neq 1 \text{ et } j \neq i \\ a_i \text{ si } j = 1 \\ a_1 \text{ si } j = i. \end{cases}$$

Par conséquent $\sigma \circ \tau_i \circ \sigma^{-1} = (a_1a_i)$. Ainsi, les deux applications mentionnées coïncident sur les τ_i. On sait, via le TD que S_n est engendré par les transpositions. Montrons que S_n est engendré par les transpositions τ_i. Considérons une transposition (ij). On a : $(ij) = (1i)(1j)(1i)$. Cela montre que les transpositions τ_i engendrent S_n. Puisque les applications φ et $\tau \mapsto \sigma \circ \tau \circ \sigma^{-1}$ coïncident sur les τ_i, elles sont égales.