L3 Mathématiques – Site Nancy, S5 – 2021/22

Algèbre 2 – Feuille 1

Généralités sur les groupes

Exercice 1. Soit G l'ensemble des transformations affines de $\mathbb{R}$ dans $\mathbb{R}$

$$g_{a,b} : x \mapsto ax + b, \quad \text{avec} a, b \in \mathbb{R},\ a \neq 0.$$

Montrer que G muni de la composition des applications, est un groupe non abélien.

Corrigé. *Soient $g_{a_1,b_1}, g_{a_2,b_2} \in G$. D'abord $\forall x \in \mathbb{R}$,*

$$\begin{aligned} g_{a_1,b_1} \circ g_{a_2,b_2}(x) &= g_{a_1,b_1}(a_2x + b_2) = a_1(a_2x + b_2) + b_1 \\ &= (a_1a_2)x + (a_1b_2 + b_1) \\ &= g_{a_1a_2,a_1b_2+b_1}(x) \end{aligned}$$

donc $g_{a_1,b_1} \circ g_{a_2,b_2} \in G$ et la loi $\circ$ est bien une LCI sur G. On voit tout de suite que cette loi n(est pas commutative, par exemple $g_{-1,1} \circ g_{1,2} = g_{-1,-1}$ et $g_{1,2} \circ g_{-1,1} = g_{-1,3}$.

- Associativité : soient $g_{a_1,b_1}, g_{a_2,b_2}, g_{a_3,b_3} \in G$. On a

$$\begin{aligned} (g_{a_1,b_1} \circ g_{a_2,b_2}) \circ g_{a_3,b_3} &= g_{a_1a_2,a_1b_2+b_1} \circ g_{a_3,b_3} \\ &= g_{a_1a_2a_3,(a_1a_2)b_3+a_1b_2+b_1} \\ &= g_{a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1} \end{aligned}$$

et

$$\begin{aligned} g_{a_1,b_1} \circ (g_{a_2,b_2} \circ g_{a_3,b_3}) &= g_{a_1,b_1} \circ g_{a_2a_3,a_2b_3+b_2} \\ &= g_{a_1a_2a_3,a_1(a_2b_3+b_2)+b_1} \\ &= g_{a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1} \end{aligned}$$

On en déduit que $(g_{a_1,b_1} \circ g_{a_2,b_2}) \circ g_{a_3,b_3} = g_{a_1,b_1} \circ (g_{a_2,b_2} \circ g_{a_3,b_3})$, d'où l'associativité.

- Neutre : il est claire que $Id_{\mathbb{R}} = g_{1,0} \in G$ et que c'est l'élément neutre pour $\circ$.

- Symétriques : soit $g_{a_1,b_1} \in G$ et cherchons $g_{a_2,b_2} \in G$ tel que $g_{a_1,b_1} \circ g_{a_2,b_2} = Id_{\mathbb{R}}$. Donc $g_{a_1a_2,a_1b_2+b_1} = Id_{\mathbb{R}} = g_{1,0}$ et $a_1a_2 = 1$, $a_1b_2 + b_1 = 0$ ce qui nous donne

$$a_2 = \frac{1}{a_1},\ b_2 = -\frac{b_1}{a_1}$$

Ainsi $g_{1/a_1,-b_1/a_1} \in G$ et $g_{a_1,b_1} \circ g_{1/a_1,-b_1/a_1} = Id_{\mathbb{R}}$. On montre de même que $g_{1/a_1,-b_1/a_1} \circ g_{a_1,b_1} = Id_{\mathbb{R}}$. On en déduit que tout élément $g_{a_1,b_1} \in G$ est symétrisable (à gauche et à droite) et que son symétrique est $g^{-1}_{a_1,b_1} = g_{1/a_1,-b_1/a_1}$. En conclusion $(G, \circ)$ est un groupe non abélien.

Exercice 2. Montrer que $\mathbb{R}^2$ muni de la loi

$$(a, b) \star (a', b') = (a + a', be^{a'} + b'e^{-a})$$

est un groupe non abélien.

Corrigé. *Il est claire que la loi $\star$ est une LCI sur $\mathbb{R}^2$ et que c'est une loi non commutative, par exemple $(1, 1) \star (1, 0) = (2, e)$ et $(1, 0) \star (1, 1) = (2, 1/e)$.*

- Associativité : soient $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ trois éléments de $\mathbb{R}^3$. On a

$$\begin{aligned} ((a_1, b_1) \star (a_2, b_2)) \star (a_3, b_3) &= (a_1 + a_2, b_1e^{a_2} + b_2e^{-a_1}) \star (a_3, b_3) \\ &= (a_1 + a_2 + a_3, (b_1e^{a_2} + b_2e^{-a_1})e^{a_3} + b_3^{-a_1-a_2}) \\ &= (a_1 + a_2 + a_3, b_1e^{a_2+a_3} + b_2e^{-a_1+a_3} + b_3^{-a_1-a_2}) \end{aligned}$$

et

$$\begin{aligned} (a_1, b_1) \star ((a_2, b_2) \star (a_3, b_3)) &= (a_1, b_1) \star (a_2 + a_3, b_2e^{a_3} + b_3e^{-a_2}) \\ &= (a_1 + a_2 + a_3, b_1e^{a_2+a_3} + (b_2e^{a_3} + b_3e^{-a_2})e^{-a_1}) \\ &= (a_1 + a_2 + a_3, b_1e^{a_2+a_3} + b_2e^{-a_1+a_3} + b_3^{-a_1-a_2}) \end{aligned}$$

On en déduit que $((a_1, b_1) \star (a_2, b_2)) \star (a_3, b_3) = (a_1, b_1) \star ((a_2, b_2) \star (a_3, b_3))$, d'où l'associativité.

- Neutre : il est claire que $(0, 0)$ est l'élément neutre de la loi $\star$.

- Symétriques : soit $(a_1, b_1) \in \mathbb{R}^2$ et cherchons $(a_2, b_2) \in \mathbb{R}^2$ tel que $(a_1, b_1) \star (a_2, b_2) = (0, 0)$. Donc $(a_1 + a_2, b_1e^{a_2} + b_2e^{-a_1}) = (0, 0)$, d'où par suite $a_2 = -a_1$ et $b_2 = -b_1$. ON en déduit que $(a_1, b_1) \star (-a_1, -b_1) = (0, 0)$ et on montre aussi que $(-a_1, -b_1) \circ (a_1, b_1)$. Par conséquent tout élément $(a_1, b_1) \in \mathbb{R}^2$ est symétrisable et son symétrique est $(a_1, b_1)^{-1} = (-a_1, -b_1) \in \mathbb{R}^2$.

En conclusion $(\mathbb{R}^2, \star)$ est un groupe non abélien.

Exercice 3. Sur $G =]-1, 1[$ on définit la loi

$$a \star b = \frac{a + b}{1 + ab}, \quad \forall x, y \in G.$$

(a) Montrer que $(G, \star)$ est un groupe abélien.

(b) En utilisant $f : x \mapsto \ln\left(\frac{1+x}{1-x}\right)$, montrer que $(G, \star)$ est isomorphe à $(\mathbb{R}, +)$.

Corrigé. *(a) Soit $a, b \in G =]-1, 1[$. On a $|ab| < 1$ et $1 + ab > 1$. Donc $a \star b$ est bien défini. De plus*

$$\begin{aligned}(a+b)^2 - (1+ab)^2 &= a^2 + b^2 - 1 - a^2b^2 \\ &= (a^1 - 1)(b^2 - 1) < 0\end{aligned}$$

donc $|a \star b| < 1$ et $a \star b \in G$. On en déduit que $\star$ est une LCI sur G (en fait c'est la question la moins évidente de l'exercice !).
De la commutativité de la somme et du produit sur $\mathbb{R}$ on déduit la commutativité de $\star$. Il est claire que 0 est l'élément neutre et que tout élément $a \in G$ est symétrisable de symétrique $a^{-1} = -a \in G$.
Vérifions maintenant l'associativité. Soient $a, b, c \in G$. On a

$$\begin{aligned}a \star (b \star c) &= \frac{a + b \star c}{1 + a(b \star c)} = \frac{a + \frac{b+c}{1+bc}}{1 + a\frac{b+c}{1+bc}} \\ &= \frac{a + b + c + abc}{ab + ac + bc + 1}\end{aligned}$$

On montre de même que

$$(a \star b) \star c = \frac{a + b + c + abc}{ab + ac + bc + 1}$$

d'où l'associativité.
En conclusion $(G, \star)$ est un groupe abélien.
(b) Soient $a, b \in G$, on a

$$\begin{aligned}f(a \star b) &= \ln\left(\frac{1 + a \star b}{1 - a \star b}\right) \\ &= \ln\left(\frac{1 + \frac{a+b}{1+ab}}{1 - \frac{a+b}{1+ab}}\right) \\ &= \ln\left(\frac{1 + ab + a + b}{1 + ab - a - b}\right) \\ &= \ln\left(\frac{(1+a)(1+b)}{(1-a)(1-b)}\right) \\ &= \ln\left(\frac{1+a}{1-a}\right) + \ln\left(\frac{1+b}{1-b}\right) \\ &= f(a) + f(b)\end{aligned}$$

Donc f est un morphisme du groupe $(G, \star)$ vers le groupe $(\mathbb{R}, +)$. De plus l'application $x \mapsto \ln\left(\frac{1+x}{1-x}\right)$ est continue et strictement croissante sur $]-1, 1[$, c'est donc une bijection de $]-1, 1[$ sur $\mathbb{R}$.
En conclusion f est un isomorphisme de $(G, \star)$ sur $(\mathbb{R}, +)$.

Exercice 4. Montrer que $\mathbb{Z}$ muni de la loi $\star$ définie par

$$a \star b = a + (-1)^a b, \ \forall a, b \in \mathbb{Z}$$

est un groupe. Est-il commutatif ?

Corrigé. *Il est claire que cette loi n'est pas commutative. Par exemple $1 \star (-1) = 2$ et $(-1) \star 1 = -2$.*
- Associativité : soient $a, b, c \in \mathbb{Z}$. Donc $a \star (b \star c) = a + (-1)^a b + (-1)^a (-1)^b c$ et $(a \star b) \star c = a + (-1)^a + (-1)^a (-1)^{(-1)^a b} c$. Or $(-1)^{(-1)^a b} = (-1)^{\pm b} = (-1)^b$, d'où $a \star (b \star c) = (a \star b) \star c$.
- Neutre : Il est claire que 0 est l'élément neutre pour $\star$, $\forall a \in \mathbb{Z}$, $a \star 0 = 0 \star a = a$.
- Symétriques : Soit $a \in \mathbb{Z}$ et cherchons $b \in \mathbb{Z}$ tel que $a \star b = 0$. Donc a donc $b = (-1)^{a+1} a \in \mathbb{Z}$. Ainsi $a \star (-1)^{a+1} a = 0$ et on vérifie aussi que $(-1)^{a+1} a \star a = 0$. Ainsi tout élément $a \in \mathbb{Z}$ est symétrisable de symétrique $a^{-1} = (-1)^{a+1} a$.
En conclusion $(\mathbb{Z}, \star)$ est un groupe non abélien.

Exercice 5. (a) Montrer qu'un groupe G où tout élément $a \in G$ est involutif c-à-d. $a^2 = e$, est abélien.
(b) Montrer que si G est d'ordre fini, alors cet ordre est une puissance de 2.

Corrigé. *(a) La propriété $a^2 = e$ est equivalence à $a^{-1} = a$. Donc dans ce groupe tout élément est son propre inverse.*
Soient $a, b \in G$, on a $ab \in G$ et $(ab)^{-1} = ab$, ce qui donne $b^{-1}a^{-1} = ab$, d"où $ba = ab$. Le groupe G est donc abélien.
(b) Supposons que G est d'ordre fini, $|G| = n < \infty$.
Si $n = 1$, alors $G = \{e\}$ et $|G| = 1 = 2^0$.
Supposons que $|G| = n > 1$. Il existe donc $a_1 \in G$ tel que $a_1 \neq e$. L'ensemble $H_1 = \{e, a_1\}$ est un sous-groupe de G d'ordre 2.
Si $H_1 = G$, alors $|G| = 2 = 2^1$;
Sinon, il existe $a_2 \in G$ tel que $a_2 \notin H_1$ (i.e. $a_2 \neq a_1$, $a_2 \neq e$). Vérifions que l'ensemble $H_2 := H_1 \cup a_2 H_1$ est un sous-groupe de G. Soient $x, y \in H_2$.
Si $x \in H_1$ et $y \in H_1$, alors $xy^{-1} \in H \subset H_2$
Si $x \in H_1$ et $y = a_2 v \in a_2 H_1$, alors $xy^{-1} = x(a_2 v)^{-1} = x a_2 v = a_2 (xv) \in a_2 H_1 \subset H_2$
Si $x \in a_2 H_1$ et $y \in H_1$, on montre de même que $xy^{-1} \in a_2 H_1 \subset H_2$;
Si $x = a_2 u \in a_2 H_1$ et $y = a_2 v \in a_2 H_1$, alors $xy^{-1} = (a_2 u)(a_2 v)^{-1} = a_2 u a_2 v = a_2^2 uv = uv \in H_1 \subset H_2$.
On en déduit que H_2 est un sous-groupe de G. L'ordre de ce sous-groupe est $|H_2| = 2|H_1| = 2^2$.
Si $H_2 = G$, alors $|G| = 2 = 2^2$; Sinon, il existe $a_3 \in G$ tels que $a_3 \notin H_2$. L'ensemble $H_3 = H_2 \cup a_3 H_2$ est un sous-groupe de G d'ordre 2^3. S'il coincide avec G, alors G est d'ordre 2^3 sinon, il existe $a_4 \in G \setminus H_3$ etc...
Comme G est d'ordre fini, ce processus s'arrête au bout d'un nombre fini d'opérations et $G = H_k$ avec $|G| = 2^k$.

Exercice 6. Soit G un groupe. Montrer que les propriétés suivantes sont équivalentes :

(1) G abélien ;
(2) $(ab)^2 = a^2b^2$ pour tout $a, b \in G$;
(3) $(ab)^{-1} = a^{-1}b^{-1}$ pour tout $a, b \in G$;
(4) $(ab)^n = a^n b^n$ pour tout $a, b \in G$ et pour tout $n \in \mathbb{Z}$;
(5) $(ab)^n = a^n b^n$ pour trois entiers n consécutifs et pour tout $a, b \in G$.
Montrer que (5) $\Rightarrow$ (1) est fausse si on remplace "trois" par "deux" dans (5).

Corrigé. (1) $\Rightarrow$ (2) $(ab)^2 = abab = a(ba)b = a(ab)b = a^2b^2$.
(2) $\Rightarrow$ (1) *$abab = (ab)^2 = a^2b^2 = aabb$ et par simplification par b à droite et a à gauche on trouve $ba = ab$.*
(1) $\Rightarrow$ (3) $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$
(3) $\Rightarrow$ (1) $ba = (b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = ((ab)^{-1})^{-1} = ab$
(1) $\Rightarrow$ (4) *On montre (4) par récurrence sur $n \geq 0$. La propriété est vraie pour $n = 0$. Soit $n \in \mathbb{N}$ et supposons que $(ab)^n = a^n b^n$. On a alors $(ab)^{n+1} = (ab)^n(ab) = a^n b^n ab = a^n ab^n b = a^{n+1}b^{n+1}$. Ainsi $\forall n \in \mathbb{N}$, $(ab)^n = a^n b^n$ et d'après (3), $\forall n \in \mathbb{Z}$, $(ab)^n = a^n b^n$.*
(4) $\Rightarrow$ (1) *évident, prendre $n = 1$.*
(4) $\Rightarrow$ (5) *évident.*
(5) $\Rightarrow$ (1) *supposons qu'il existe $m \in \mathbb{Z}$ tels que $(ab)^{m+k} = a^{m+k}b^{m+k}$ pour $k = 0, 1, 2$. On a $a^{m+1}b^{m+1} = (ab)^{m+1} = (ab)^m(ab) = a^m b^m ab$. En multipliant cette égalité par l'inverse de a^m à gauche et l'inverse de b à droite on trouve $ab^m = b^m a$. De même $bab^{m+1}a^{m+1} = (ba)(ba)^{m+1} = (ba)^{m+2} = b^{m+2}a^{m+2}$, d'où $ab^{m+1} = b^{m+1}a$. En utilisant les deux identités trouvées on a $bab^m = b(ab^m) = b(b^m a) = b^{m+1}a = ab^{m+1}$ et en multipliant par l'inverse de b^m à droite on trouve $ba = ab$. On en déduit que G est abélien.*
Si au lieu de (5) on a (5') $(ab)^n = a^n b^n$ pour deux entiers n consécutifs, alors (5') $\Rightarrow$ (1) est fausse. Exemple : $G = \mathcal{S}_3$ est un groupe non abélien car $(1\,2)(1\,2\,3) = (2\,3)$ mais $(1\,2\,3)(1\,2) = (1\,3)$. Cependant $\forall \sigma, \tau \in S_3$, $(\sigma\tau)^0 = e = \sigma^0\tau^0$ et $(\sigma\tau)^1 = \sigma\tau = \sigma^1\tau^1$.

Exercice 7. Donner un exemple d'un groupe non abélien G tel que $a, b \in G$ on ait $(ab)^3 = a^3b^3$, pour tout $a, b \in G$. Indication : considérer les éléments a de $\mathcal{M}(3, \mathbb{Z}/3\mathbb{Z})$ tels que $a_{i,i} = \bar{1}$ pour $1 \leq i \leq 3$ et $a_{i,j} = \bar{0}$ pour $1 \leq j < i \leq 3$.

Corrigé. *Le groupe*

$$G = \left\{ A = \begin{pmatrix} \bar{1} & \bar{a} & \bar{b} \\ \bar{0} & \bar{1} & \bar{c} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \ : \ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/3\mathbb{Z} \right\}$$

est un groupe non abélien (à vérifier). Si $A = \begin{pmatrix} \bar{1} & \bar{a} & \bar{b} \\ \bar{0} & \bar{1} & \bar{c} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in G$ on a

$$A^3 = \begin{pmatrix} \bar{1} & \bar{3}\bar{a}\bar{c} & \bar{3}\bar{b} \\ \bar{0} & \bar{1} & \bar{3}\bar{c} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = I_3$$

On en déduit que $\forall A, B \in G$, $(AB)^3 = A^3B^3$.

Exercice 8. Soit H et K deux sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subseteq K$ ou $K \subseteq H$.

Corrigé. *Il est claire que si $H \subset K$ ou $K \subset H$ alors $H \cup K$ est un sous-groupe de G.*
Réciproquement, supposons que $H \cup K$ est un sous-groupe de G. Supposons par l'absurde que $H \not\subseteq K$ et $K \not\subseteq H$. Alors il existe $x \in K$ tel que $x \notin H$ et $y \in H$ tel que $y \notin K$. Comme $x, y \in H \cup K$ et que $H \cup K$ est un sous-groupe, $xy \in H \cup K$. Si $xy \in H$, alors, puisque $y \in H$, on aurait $x = (xy)y^{-1} \in H$ ce qui est contraire à l'hypothèse ;
Si $xy \in K$, alors, puisque $x \in K$, on auarit $y = x^{-1}(xy) \in K$ ce qui est contraire à l'hypothèse.
Ceci prouve que $H \subseteq K$ ou $K \subseteq H$.

Exercice 9. Montrer que $H = \{a + b\sqrt{2}, \ \ a, b \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{R}, +)$.

Corrigé. *On a :*
$H \subset \mathbb{R}$.
$H \neq \emptyset$ car le neutre de $\mathbb{R}$, $0 = 0 + 0\sqrt{2} \in H$.
Soient $x = a + b\sqrt{2}$ et $x' = a' + b'\sqrt{2}$ deux éléments de H. On a

$$x - x' = (a - a') + (b - b')\sqrt{2} \in H$$

On en déduit que H est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 10. Montrer que $H = \{a + b\sqrt{3}, \ a \in \mathbb{N}, b \in \mathbb{Z}, a^2 - 3b^2 = 1\}$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Corrigé. *On a :*
$1 = 1 + 0\sqrt{3} \in H$, donc $H \neq \emptyset$ (remarquez que 1 est le neutre de $\mathbb{R}_+^*$).
Soit $x = a + b\sqrt{3} \in H$, alors $a^2 - 3b^2 = 1$ et $a = \sqrt{1 + 3b^2} > \sqrt{3}|b| \geq 0$. D'où

$$x = a + b\sqrt{3} > \sqrt{3}(|b| + b) \geq 0$$

Ainsi $H \subset \mathbb{R}_+^*$.
Soit $x = a + \sqrt{3}b \in H$. On a

$$\frac{1}{x} = \frac{1}{a + \sqrt{3}b} = \frac{a - b\sqrt{3}}{a^2 - 3b^3} = a - b\sqrt{3} \in H$$

Donc tout élément de $x = a + \sqrt{3}b \in H$ est inversible d'inverse $x^{-1} = a - b\sqrt{3}$. Soient $x = a + b\sqrt{3}$ et $x' = a' + b'\sqrt{3}$ deux éléments de H. On a

$$xx' = (a + b\sqrt{3})(a' + b'\sqrt{3}) = (aa' + 3bb') + (ab' + ba')\sqrt{3}$$

avec $aa' + 3bb' \in \mathbb{Z}$ et $ab' + ba') \in \mathbb{Z}$. Or

$$\begin{aligned}(aa' + 3bb')^2 - 3(ab' + ba')^2 &= a^2a'^2 + 9b^2b'^2 - 3a^2b'^2 - 3b^2a'^2 \\ &= a^2(a'^2 - 3b'2) - 3b^2(a'^2 - 3b'^2) \\ &= a^2 \times 1 - 3b^2 \times 1 \\ &= 1\end{aligned}$$

Pour pouvoir dire que xx' est dans H il reste à vérifier que $aa' + 3bb' \in \mathbb{N}$. Or d'après ce qui précède, $a > \sqrt{3}|b|$ et $a' > \sqrt{3}|b'|$, donc $aa' > 3|bb'|$ et $aa' + 3bb' > 3(bb' + |bb'|) \geq 0$. Finalement $xx' \in H$.

Exercice 11. Montrer que

$$H = \{\begin{pmatrix} 2^k & \frac{n}{2^m} \\ 0 & 2^{-k} \end{pmatrix} | k, n, m \in \mathbb{Z}\}$$

est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

Corrigé. *Il est claire que $H \subset \mathrm{GL}(2, \mathbb{R})$, puisque toute matrice de H est inversible. De plus l'élément neutre I_2 de $\mathrm{GL}(2, \mathbb{R})$ est dans H.*
Soient $x = \begin{pmatrix} 2^k & \frac{n}{2^m} \\ 0 & 2^{-k} \end{pmatrix}$ et $x' = \begin{pmatrix} 2^{k'} & \frac{n'}{2^{m'}} \\ 0 & 2^{-k'} \end{pmatrix}$ deux éléments de H. On a

$$\begin{aligned}xx'^{-1} &= \begin{pmatrix} 2^k & \frac{n}{2^m} \\ 0 & 2^{-k} \end{pmatrix} \begin{pmatrix} 2^{-k'} & -\frac{n'}{2^{m'}} \\ 0 & 2^{k'} \end{pmatrix} \\ &= \begin{pmatrix} 2^{(k-k')} & \frac{n2^{m'-k} - n'2^{m-k'}}{2^{m+m'-k-k'}} \\ 0 & 2^{-(k-k')} \end{pmatrix} \in H\end{aligned}$$

Ainsi H est un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

Exercice 12. Montrer que

$$H = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ; \ a, b, c \in \mathbb{R}\}$$

est un sous-groupe de $\mathrm{GL}(3, \mathbb{R})$.

Corrigé. *Même raisonnement que dans l'exercice précédent. Laissé au lecteur.*

Exercice 13. Soit H un sous-groupe strict d'un groupe G. Déterminer le groupe engendré par le complémentaire de H dans G.

Corrigé. *Soit $H \subsetneq G$ un sous-groupe strict de G et soit $H^c = G \setminus H$ son complémentaire dans G. Il faut noter que H^c n'est pas un sous-groupe de G (par exemple, ne contient pas le neutre de G). Notons aussi que $G = H \cup H^c$. Montrons que le sous-groupe $\langle H^c \rangle$ engendré par H^c coincide avec G.*
D'abord $\langle H^c \rangle \subset G$.
Inversement, on a $H^c \subset \langle H^c \rangle$. Il suffit alors de montrer que $H \subset \langle H^c \rangle$.
Comme $H \subsetneq G$, on a $H^c \neq \emptyset$ et H^c contient au moins un élément $a \in H^c$.
Soit $x \in H$, alors $ax \notin H$, car sinon on aurait $a = (ax)x^{-1} \in H$ ce qui est contraire à l'hypothèse.
Donc $ax \in H^c$ et

$$x = \underbrace{(a^{-1})}_{\in \langle H^c \rangle} \underbrace{(ax)}_{\in \langle H^c \rangle} \in \langle H^c \rangle$$

Ainsi $H \subset \langle H^c \rangle$ et $G = H \cup H^c \subset \langle H^c \rangle$. En conclusion $\langle H^c \rangle = G$

Exercice 14. Soit G un groupe multiplicatif.
(a) Montrer que pour tout élément $a \in G$, le centralisateur de a,

$$Z_a = \{b \in G, \ \ ab = ba\}$$

est un sous-groupe de G.
(b) Montrer que le centre de G,

$$Z(G) = \{a \in G, \ \ \forall b \in G, \ ab = ba\}$$

est un sous-groupe de G.
(c) Déterminer les centres des groupes $GL(n, \mathbb{R})$ et $SL(n, \mathbb{R})$.

Corrigé.
(a) On a $Z_a \neq \emptyset$ puisque $e \in Z_a$. Soient $a, y \in Z_a$, on a

$$\begin{aligned}(xy)a &= x(ya) = x(ay) \\ &= (xa)y = (ax)y = a(xy)\end{aligned}$$

donc $xy \in Z_a$.
Pour $x \in Z_a$, on a $ax = xa$ donc

$$x^{-1}a = x^{-1}axx^{-1} = x^{-1}xax^{-1} = ax^{-1}$$

Ainsi $x^{-1} \in Z_a$.
On en déduit que Z_a est un sous-groupe de G, c'est en fait un sous-groupe distingué de G.
(b) On peut montrer de la même façon que le centre de G, $Z(G)$ est un sous-groupe (distingué) de G. On peut aussi remarquer que

$$Z(G) = \bigcap_{a \in G} Z_a$$

et comme l'intersection de sous-groupes (distingués) de G est un sous-groupe (distingué) de G, le centre $Z(G)$ est un sous-groupe (distingué) de G.

(c) Soit $A = (a_{i,j}) \in Z(GL(n,\mathbb{R}))$. Donc pour tout $M \in Z(GL(n,\mathbb{R}))$, $MA = AM$. Soit $E_{i,j}$ avec $i \neq j$ une matrice élémentaire (élément de la base canonique de $\mathcal{M}_n(\mathbb{R})$, alors $I_n + E_{i,j} \in GL(n,\mathbb{R})$. La relation de commutation donne $(I_n + E_{i,j})A = A(I_n + E_{i,j})$, d"où $AE_{i,j} = E_{i,j}A$. En désignat par $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{R}^n$, on a

$$\begin{cases} (AE_{i,j})e_j = Ae_i = \sum_{k=1}^n a_{k,i}e_k \\ (E_{i,j}A)e_j = E_{i,j}(Ae_j) = E_{i,j}\left(\sum_{k=1}^n a_{kj}e_k\right) = a_{j,j}e_i \end{cases}$$

Donc

$$\sum_{k=1}^n a_{k,i}e_k = a_{j,j}e_i$$

d'où

$$\begin{cases} a_{k,i} = 0 & \text{pour } k \in \{1,\cdots,n\} - \{i\} \\ a_{i,i} = a_{j,j} & \text{pour } k = i \end{cases}$$

On en déduit que les coefficients diagonaux de A sont tous égaux, et on note $\forall i, a_{i,i} = \lambda$ la valeur commune. Ainsi, A est une homothétie,

$$A = \text{diag}(\lambda,\cdots,\lambda) = \lambda I_n, \quad \lambda \in \mathbb{R}^*$$

Réciproquement, ces matrices d'homothéties sont bien dans le centre de $GL(n,\mathbb{R})$. En conclusion

$$Z(GL(n,\mathbb{R})) = \{\lambda I_n \mid \lambda \in \mathbb{R}^*\}.$$

Comme les matrices $I_n + E_{i,j}$ (pour $i \neq j$) sont aussi dans $SL(n,\mathbb{R})$, le raisonnement précédent montre que le centre de $SL(n,\mathbb{R})$

$$Z(SL(n,\mathbb{R})) = \begin{cases} \{I_n\} & \text{si } n \text{ impair} \\ \{-I_n, I_n\} & \text{si } n \text{ pair} \end{cases}$$

Exercice 15. Quels sont les éléments du sous-groupe engendré par $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ dans $\text{GL}(2,\mathbb{R})$.

Corrigé. *Soit $a = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, qui est une matrice inversible, donc élément de $\text{GL}(2,\mathbb{R})$. Le sous-groupe de $\text{GL}(2,\mathbb{R})$ engendré par a est*

$$H = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Déterminons donc les différentes puissances de a. On a

$$a^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, a^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

On peut en déduire directement que $a^6 = I_2$ et que a est d'ordre 6. Ainsi

$$H = \langle a \rangle = \{I_2, a, a^2, a^3, a^4, a^5\}$$

Exercice 16. Soit G un groupe fini. Montrer que pour tout $a, b \in G$ on a :
(a) a et a^{-1} ont le même ordre ;
(b) a et bab^{-1} ont le même ordre ;
(c) ab et ba ont le même ordre.

Corrigé. *(a) Si $o(a) = n$ alors $a^n = e$ et $(a^{-1})^n = (a^n)^{-1} = e$. D'où $o(a^{-1})$ divise $o(a)$. En échangeant les rôles de a et a^{-1}, on déduit que divise $o(a)$ divise $o(a^{-1})$. Ainsi $o(a^{-1}) = o(a)$.*

(b) Si $o(a) = n$ alors $(bab^{-1})^n = ba^nb^{-1} = beb^{-1} = e$. Donc $o(bab^{-1})$ divise $o(a)$. D'après ce qui précède, $o(a) = o(b^{-1}(bab^{-1})b)$ divise $o(bab^{-1})$. D'où $o(bab^{-1}) = o(a)$.

(c) On a $ba = b(ab)b^{-1}$, donc d'après la question précédente $o(ba) = o(b(ab)b^{-1}) = o(ab)$.

Exercice 17. Montrer que dans un groupe abélien G, l'ensemble des éléments d'ordre fini forme un sous-groupe de G

Corrigé. *Soit $H = \{x \in G \mid o(x) < \infty\}$ l'ensemble des éléments d'ordre fini de G. H est évidemment non vide car il contient e. Soient $x, y \in H$, alors il existe $k, h \in \mathbb{N}$ tel que $x^k = e$ et $y^h = e$. Comme G est abélien, an a*

$$(xy)^{kh} = x^{kh}y^{kh} = (x^k)^h(y^h)^k = e^he^k = e$$

Donc xy est d'ordre fini et $xy \in H$. D'où la stabilité de H par le produit.
D'après l'exercice précédent, si x est d'ordre fini, alors x^{-1} est aussi d'ordre fini.
D'où la stabilité de H par le passage à l'inverse.
En conclusion H est un sous-groupe de G.

Exercice 18. Soit G un groupe abélien et a et b deux éléments d'ordre fini.

(a) Montrer que ab est d'ordre fini et que l'ordre de ab divise le ppcm des ordres de a et b.

(b) Montrer que si les ordres de a et b sont premiers entre eux, l'ordre de ab est égal au ppcm des ordres de a et b.

Corrigé. *(a) D'après l'exercice précédent, si a et b sont d'ordre fini, alors ab est d'ordre fini (on rappelle que G est abélien).*
Soit $o(a) = n$ et $o(b) = m$ et soit $d = \text{ppcm}(n,m)$. Comme G est abélien, an a $(ab)^d = a^db^d = ee = e$ Donc $o(ab)$ divise $d = \text{ppcm}(o(a), o(b))$

(b) Supposons que $o(a) = n$ et $o(b) = m$ sont premiers entre eux et soit $k \in \mathbb{Z}$ tel que $(ab)^k = e$. Alors $a^b = b^{-k}$ et $e = (a-n)^k = a^{nk} = b^{-nk}$, d'où m divise

nk. Comme m et n sont premiers entre eux, m divise k. On montre de même que n divise k. Par conséquent mn divise k et $o(ab) = mn = \text{ppcm}(n,m)$. En conclusion si $o(a)$ et $o(b)$ sont premiers entre eux alors $o(ab) = o(a)o(b)$.

Exercice 19. (a) Montrer que $\text{SL}(2,\mathbb{Z})$ est un groupe multiplicatif.

(b) On considère les deux éléments $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ du groupe $\text{SL}(2,\mathbb{Z})$.

Montrer que a et b sont d'ordres finis mais que ab est d'ordre infini.

Corrigé. *Montrons que $\text{SL}(2,\mathbb{Z})$ est un sous-groupe de $GL(2,\mathbb{R})$.*
On a :
$\text{SL}(2,\mathbb{Z}) \subset GL(2,\mathbb{R})$;
$I_2 \in \text{SL}(2,\mathbb{Z})$;
Si A et B sont deux matrices de $\text{SL}(2,\mathbb{Z})$ alors elles sont à coefficients entiers et de déterminant égal à 1. Le produit AB est clairement à coefficients entiers et de déterminant égal à 1. Donc $AB \in \text{SL}(2,\mathbb{Z})$.

Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2,\mathbb{Z})$ alors A est inversible car de determinant égal à 1. Elle est donc inversible dans $GL(2,\mathbb{R})$ et d'inverse,

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \text{SL}(2,\mathbb{Z})$$

D'où la stabilité par passage à l'inverse.
Notez que le groupe $SL(2,\mathbb{Z})$ (comme $GL(2,\mathbb{R})$) n'est pas abélien.

Exercice 20. Soit H le groupe engendré par les deux matrices

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Montrer qu'il est d'ordre 8 isomorphe au groupe diédral Le groupe $\mathbb{D}_4$.

Corrigé. On Montre que $a^4 = I_2$ et que $o(a) = 4$ On montre aussi que $b^2 =_2$ et que $o(b) = 2$, donc

$$\begin{aligned} H &= \{I_2, a, a^2; a^3, b, ab, a^2b, a^3b\} \\ &= \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\} \end{aligned}$$

est d'ordre 8.

En fait $a = R(90°)$ matrice de rotation qui tourne le plan de 90° et $b = T_{1,3}$ la reflexion par rapport à la diagonale $y = -x$. On considère l'application f$D_8 \to H$ définie par

$$f = \begin{pmatrix} I & R & R^2 & R^3 & T_{1,3} & TT_{1,3} & R^2T_{1,3} & R^3T_{1,3} \\ I & a & a^2 & a^3 & b & ab & a^2b & a^3b \end{pmatrix}$$

ou encore

$$f(R^iT_{1,3}^j) =^i b^j$$

f est un morphisme de groupes car

$$\begin{aligned} f(R^iR^j) &= f(R^{i+j}) = a^{i+j} = a^ia^j \\ &= f(R^i)f(R^j) \\ f((R^iT_{1,3})(R^jT_{1,3})) &= f(R^{i-j}T_{i,3}) = a^{i-j}b = (a^ib)(a^jb) \\ &= f(R^iT_{1,3})f(R^jT_{1,3}) \end{aligned}$$

De plus f est bijectif.
En conclusion $H \simeq D_4$.

Exercice 21. Montrer que $\text{SL}(n,\mathbb{R})$ est un sous-groupe distingué de $\text{GL}(n,\mathbb{R})$ et que $\text{GL}(n,\mathbb{R})/\text{SL}(n,\mathbb{R})$ est isomorphe $\mathbb{R}^*$.

Corrigé. L'application $f : GL(n,\mathbb{R}) \to \mathbb{R}^*$ définie par $f(A) = \det(A)$ est un morphisme de groupes. Si $\lambda \in \mathbb{R}^*$, alors en posant $A = \text{diag}(\lambda, 1, \cdots, 1)$, on a $\det(A) = \lambda$. On en déduit que f est surjectif. De plus $\text{Ker}(f) = \{A \in GL(n;\mathbb{R}) \mid f(A) = 1\} = \{A \in GL(n;\mathbb{R}) \mid \det(A) = 1\} = 1 = SL(n,\mathbb{R})$. Donc d'après le théorème d'isomorphisme,

$$GL(n,\mathbb{R})/SL(n,\mathbb{R}) \simeq \mathbb{R}^*.$$

Exercice 22. Soit H un sous-groupe d'indice 2 dans un groupe G. Montrer que H est distingué dans G.

Corrigé. Comme $[G : H] = 2$, le cardinal de l'ensemble quotient G/H est 2. Cet ensemble quotient contient ne contient que deux classes. La classe de e (à gauche ou à droite) est H. L'autre classe est nécessairement H^c, le complémentaire de H. Cette dernière coincide avec la classe (à gauche ou à droite) de tout élément $g \in H^c$,

$$G/H = \{H, H^c\}$$

On en déduit que $\forall g \in G$,
– si $g \in H$, il est claire que $gH = Hg$ qui n'est autre que H,
– si $g \notin H$, $gH = H^c = Hg$.
En conclusion H est distingué dans G.

Exercice 23. Soient G un groupe et H, K deux sous-groupes de G. Montrer qu'on a équivalence entre :

(a) HK est un sous-groupe de G, (c) $HK \subset KH$,

(b) KH est un sous groupe de G, (d) $KH \subset HK$.

Corrigé. (b)⇒(c) Soit $hk \in HK$, alors $k^{-1}h^{-1} \in KH$ et comme ce dernier est un sous-groupe $hk = (k^{-1}h^{-1})^{-1} \in KH$. Donc $HK \subset KH$.

(c)⇒(b) Soient $k_1h_1 \in KH$ et $k_2h_2 \in KH$. Donc $(k_1h_1)(k_2h_2) = k_1(h_1k_2)h_2$. Or $h_1k_2 \in HK \subset KH$, il existe alors $k_3 \in K, h_3 \in H$ tels que $h_1k_2 = k_3h_3$. D'où $(k_1h_1)(k_2h_2) = k_1(h_1k_2)h_2 = k_1(k_3h_3)h_2 = (k_1k_3)(h_3h_2) \in KH$. D'où la stabilité de KH par le produit.
Si $k_1h_1 \in KH$, alors $(k_1h_1)^{-1} = h_1^{-1}k_1^{-1}$ et comme $h_1^{-1}k_1^{-1} \in HK \subset KH$, il existe $k_2 \in K, h_2 \in H$ tels que $h_1^{-1}k_1^{-1} = k_2h_2$. Donc $(k_1h_1)^{-1} = k_2h_2 \in KH$. D'où la stabilité de KH par passage à l'inverse. On en déduit que KH est un sous-groupe de G.

(a)⇔(d) Découle des deux implications précédentes en échangeant H et K : H et K jouent le même rôle.

(c)⇔(d) Soit $k_1h_1 \in KH$. On a $k_1h_1 = (h_1^{-1}k_1^{-1})^{-1}$. Or $h_1^{-1}k_1^{-1} \in HK \subset KH$, donc il existe $k_2 \in K, h_2 \in H$ tels que $h_1^{-1}k_1^{-1} = k_2h_2$ et $k_1h_1 = (h_1^{-1}k_1^{-1})^{-1} = (k_2h_2)^{-1} = h_2^{-1}k_2^{-1} \in HK$. Ainsi $KH \subset HK$.

(d)⇔(c) Découle de l'implication précédente en échangeant H et K : H et K jouent le même rôle.

Exercice 24. Soient G un groupe et H, K deux sous-groupes distingués de G. On suppose que $HK = G$ et $H \cap K = \{e\}$. Montrer que $G \simeq H \times K$.

Exercice 25. Soient G un groupe et H, K deux sous-groupes de G. On suppose que K est distingué dans G. Montrer

(a) $KH = HK$ est un sous-groupe de G, K est un sous-groupe distingué de KH et $K \cap H$ est un sous-groupe distingué de H.

(b) Les deux groupes quotient KH/K et $H/K \cap H$ sont isomorphes.

Exercice 26. Soient G un groupe, H et K deux sous-groupes distingués de G tels que $K \subset H$. Montrer

(a) H/K est un sous-groupe distingué de G/K.

(b) Les deux groupes quotient $(G/K)/(H/K)$ et G/H sont isomorphes.