DS 4
Suites - Groupes, Anneaux, Corps
Correction

Simon Dauguet
simon.dauguet@gmail.com

Mercredi 04 Décembre 2024

Problème 1 (Équivalent de Stirling) :

Partie I : Un équivalent à une constante près

On considère la suite (u_n) définie par
$$\forall n \in \mathbb{N}^*,\ u_n = \frac{n!e^n}{n^n\sqrt{n}}.$$

1. On sait que $\forall n \geq 1$, $e^n > 0$, $n! \geq 1$, $\sqrt{n} \geq 1$ par croissance de la fonction racine, $n^n \geq 1$. Donc $\forall n \geq 1$, $u_n > 0$.
2. Soit $n \in \mathbb{N}^*$. On calcul :
$$\begin{aligned}\frac{u_{n+1}}{u_n} &= \frac{(n+1)!e^{n+1}}{\sqrt{n+1}(n+1)^{n+1}}\frac{\sqrt{n}n^n}{n!e^n}\\ &= e\sqrt{\frac{n}{n+1}}\left(\frac{n}{n+1}\right)^n\\ &= e^{1-\frac{1}{2}\ln(1+1/n)+n(\ln(n)-\ln(n+1))}\\ &= e^{1-\frac{1}{2}\ln(1+1/n)-n\ln(1+1/n)}\\ &= e^{1-\left(\frac{1}{2}+n\right)\ln(1+1/n)}\end{aligned}$$

3. On pose
$$\begin{aligned}\forall t > 0,\ \varphi(t) &= 1-\left(\frac{1}{2}+\frac{1}{t}\right)\ln(1+t)\\ &= \frac{2t-(t+2)\ln(1+t)}{2t}\\ &= \frac{\psi(t)}{2t}\end{aligned}$$

On remarque aussi immédiatement que
$$\forall n \in \mathbb{N}^*,\ \frac{u_{n+1}}{u_n} = e^{\varphi(1/n)}.$$

(a) ψ est infiniment dérivable sur $\mathbb{R}_+$ et
$$\forall t \in \mathbb{R}_+,\ \psi'(t) = 2-\ln(1+t)-\frac{t+2}{t+1}$$
et
$$\forall t \in \mathbb{R}_+, \psi''(t) = -\frac{1}{1+t}-\frac{t+1-t-2}{(t+1)^2} = -\frac{t}{(t+1)^2} \leq 0.$$
On en déduit le tableau de signes :

t	0 $\qquad\qquad$ $+\infty$
$\psi''(t)$	$-$
ψ'	$0 \searrow -\infty$
$\psi'(t)$	$-$
ψ	$0 \searrow -\infty$
$\psi(t)$	$-$

(b) Comme $\forall t > 0,\ \varphi(t) = \frac{\psi(t)}{2t}$, on en déduit que φ et ψ sont du même signe. Donc $\forall t > 0,\ \varphi(t) < 0$.

(c) On en déduit également que

$$\forall n \in \mathbb{N}^*,\ \frac{u_{n+1}}{u_n} = e^{\varphi(1/n)} < 1$$

par croissance de l'exponentielle. Et donc la suite (u_n) est décroissante.

4. La suite (u_n) est donc décroissante et minorée par 0 (cf question 1). Donc, par théorème de la limite monotone, elle est convergente. Donc $\lim_{n\to+\infty} u_n$ existe. On pose $C = \lim_{n\to+\infty} u_n$.

5. On sait que $\forall n \geq 1,\ u_n > 0$. Donc, par passage à la limite dans les inégalités, $C = \lim_{n\to+\infty} u_n \geq 0$.

6. On suppose $C = 0$. On pose

$$\forall n \geq 1,\ v_n = \ln(u_n).$$

(a) Comme la suite (u_n) converge vers 0 et comme $\ln(x) \xrightarrow[x\to 0]{} -\infty$. Par caractérisation séquentielle des limites (ou par composition dans les limites), on obtient $v_n = \ln(u_n) \xrightarrow[n\to+\infty]{} -\infty$. Donc la suite (v_n) est divergente vers $-\infty$.

(b) D'après la question 2, on a $\forall n \geq 2,\ v_{n+1} - v_n = \ln(u_{n+1}/u_n) = \varphi(1/n) = 1 - \left(\frac{1}{2} + n\right)\ln(1 + 1/n)$.

(c) On considère les fonctions f et g définies sur $\mathbb{R}_+$ par $f(x) = \ln(1+x) - x + x^2/2$ et $g(x) = f(x) - x^3/3$. Alors f et g sont dérivable sur $\mathbb{R}_+$ comme sommes (et composées) d'applications dérivables sur $\mathbb{R}_+$ et

$$\forall x \geq 0,\ f'(x) = \frac{1}{1+x} - 1 - x = \frac{1 - 1 - x + x + x^2}{1+x} = \frac{x^2}{1+x} \geq 0$$

et

$$\forall x \geq 0,\ g'(x) = f'(x) - x^2 = \frac{x^2 - x^2 - x^3}{1+x} = \frac{-x^3}{1+x} \leq 0.$$

Donc f est croissante sur $\mathbb{R}_+$ et g est décroissante sur $\mathbb{R}_+$. Or $f(0) = g(0) = 0$. On en déduit donc

$$\forall x \geq 0,\ x - \frac{x^2}{x} \leq \ln(1+x) \leq x - \frac{x^2}{2} + \frac{x^3}{3}.$$

(d) En particulier, $\forall n \geq 2$,

$$\frac{1}{n} - \frac{1}{2n^2} \leq \ln(1 + 1/n) \leq \frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3}.$$

On en déduit donc

$$\forall n \geq 2,\ 1 - \frac{1}{2n} \leq n\ln(1 + 1/n) \leq 1 - \frac{1}{2n} + \frac{1}{3n^2}.$$

Et aussi

$$\forall n \geq 2,\ \frac{1}{2n} - \frac{1}{4n^2} \leq \frac{1}{2}\ln(1 + 1/n) \leq \frac{1}{2n} - \frac{1}{4n^2} + \frac{1}{6n^3}.$$

En sommant les deux relations précédentes, on a

$$\forall n \geq 2,\ 1 - \frac{1}{4n^2} \leq \left(\frac{1}{2} + n\right) \ln(1 + 1/n) \leq 1 + \frac{1}{12n^2} + \frac{1}{6n^3}.$$

D'où

$$\forall n \geq 2,\ -\frac{1}{12n^2} - \frac{1}{6n^3} \leq 1 - \left(\frac{1}{2} + n\right) \ln(1 + 1/n) = v_{n+1} - v_n \leq \frac{1}{4n^2}.$$

(e) En sommant les inégalités précédentes, on trouve, par télescopage,

$$\begin{aligned} \forall n \geq 2,\ -\frac{1}{12}\sum_{k=2}^{n} \frac{1}{k^2} - \frac{1}{6}\sum_{k=2}^{n} \frac{1}{k^3} &\leq \sum_{k=2}^{n} (v_{k+1} - v_k) \\ &= v_{n+1} - v_2 \\ &\leq \frac{1}{4}\sum_{k=2}^{n} \frac{1}{k^2}. \end{aligned}$$

(f) Or

$$\sum_{k=2}^{n} \frac{1}{k^2} \xrightarrow[n \to +\infty]{} \zeta(2) - 1 = \frac{\pi^2}{6} - 1 \in \mathbb{R}$$

et

$$\sum_{k=2}^{n} \frac{1}{k^3} \xrightarrow[n \to +\infty]{} \zeta(3) - 1 \in \mathbb{R}.$$

Donc $(v_{n+1} - v_2)_{n\in\mathbb{N}}$ est une suite minorée (encadrée par deux suites convergentes, donc deux suites bornées). Or par hypothèse, $u_n \xrightarrow[n \to +\infty]{} 0$, donc par composition dans les limites, $v_n = \ln(u_n) \xrightarrow[n \to +\infty]{} -\infty$. Et donc (v_n) n'est pas minorée. D'où ☠.

On en conclut que $C \neq 0$. Or $C \geq 0$. Donc $C > 0$.

7. Comme $u_n \xrightarrow[n \to +\infty]{} C \neq 0$, on en déduit $u_n \underset{n \to +\infty}{\sim} C$. Et par multiplication, on a immédiatement,

$$n! \underset{n \to +\infty}{\sim} C\sqrt{n}\left(\frac{n}{e}\right)^n.$$

Partie II

On considère la suite $(I_n)_{n\in\mathbb{N}}$ définit par

$$\begin{cases} I_0 = \frac{\pi}{2} \\ I_1 = 1 \\ \forall n \in \mathbb{N},\ I_{n+2} = \frac{n+1}{n+2} I_n \end{cases}$$

que l'on admet être décroissante et strictement positive.

8. On a alors

$$I_2 = \frac{1}{2} I_0 = \frac{\pi}{4}$$

et

$$I_3 = \frac{1+1}{1+2} I_1 = \frac{2}{3}$$

et

$$I_4 = \frac{2+1}{2+2} I_2 = \frac{3\pi}{16}$$

et

$$I_5 = \frac{3+1}{3+2} I_3 = \frac{4}{5} \times \frac{2}{3} = \frac{8}{15}$$

9. Soit $n \in \mathbb{N}$. Alors

$$J_{n+1} = (n+2)I_{n+2}I_{n+1} = (n+2)\frac{n+1}{n+2}I_nI_{n+1} = (n+1)I_nI_{n+1} = J_n$$

Donc la suite $(J_n)_{n\in\mathbb{N}}$ constante égale à $J_0 = I_0I_1 = \frac{\pi}{2}$.

10. On pourrait montrer les relations par récurrences, mais on va faire autrement. On sait que

$$\forall n \in \mathbb{N},\ I_{2n+2} = \frac{2n+1}{2n+2}I_{2n} = \frac{2(n+1)-1}{2(n+1)}I_{2n}$$

Et par une récurrence facile, on a alors

$$\forall n \in \mathbb{N},\ I_{2n} = \prod_{k=1}^{n}\frac{2k-1}{2k}I_0$$

D'où l'on déduit alors, $\forall n \in \mathbb{N}$,

$$\begin{aligned} I_{2n} &= \frac{\prod_{k=1}^{n}(2k-1)}{\prod_{k=1}^{n}2k}I_0 \\ &= \frac{\prod_{k=1}^{n}\frac{2k(2k-1)}{2k}}{2^n\prod_{k=1}^{n}k}\frac{\pi}{2} \\ &= \frac{\frac{\prod_{k=1}^{2n}k}{\prod_{k=1}^{n}2k}}{2^n n!}\frac{\pi}{2} \\ &= \frac{(2n)!}{(2^n n!)^2}\frac{\pi}{2} \end{aligned}$$

Et de même, on a

$$\forall n \in \mathbb{N},\ I_{2n+3} = \frac{2n+2}{2n+3}I_{2n+1} = \frac{2(n+1)}{2(n+1)+1}I_{2n+1}$$

Donc, par récurrence facile, $\forall n \in \mathbb{N}$,

$$\begin{aligned} I_{2n+1} &= \prod_{k=1}^{n}\frac{2k}{2k+1}I_1 \\ &= \frac{2^n n!}{\prod_{k=1}^{n}(2k+1)} \\ &= \frac{2^n n!}{\prod_{k=1}^{n}\frac{2k(2k+1)}{2k}} \\ &= \frac{(2^n n!)^2}{(2n+1)!} \end{aligned}$$

11. On sait que $(I_n)_{n\in\mathbb{N}}$ est décroissante. Donc $\forall n \in \mathbb{N}^*$, $I_{n-1} \leq I_n \leq I_{n+1}$. Mais comme $\forall n \in \mathbb{N}$, $I_n > 0$, on a donc $\forall n \in \mathbb{N}^*$, $\frac{I_{n-1}}{I_{n+1}} \leq \frac{I_n}{I_{n+1}} \leq 1$. Mais en utilisant la relation de récurrence vérifiée par (I_n), on en déduit donc $\forall n \in \mathbb{N}^*$, $\frac{n+1}{n} = 1 + \frac{1}{n} \leq \frac{I_n}{I_{n+1}} \leq 1$. Or $1 + \frac{1}{n} \xrightarrow[n\to+\infty]{} 1$, donc par théorème des gendarmes, $\frac{I_n}{I_{n+1}} \xrightarrow[n\to+\infty]{} 1$ et donc $I_n \underset{n\to+\infty}{\sim} I_{n+1}$.

12. On rappelle que $\forall n \in \mathbb{N}$, $J_n = (n+1)I_{n+1}I_n = \frac{\pi}{2}$. Donc $J_n \underset{n\to+\infty}{\sim} \frac{\pi}{2}$ puisque $\pi/2 \neq 0$ et $J_n = (n+1)I_nI_{n+1} \underset{n\to+\infty}{\sim} nI_n^2$.

On en déduit donc, par transitivité de la relation d'équivalence, $nI_n^2 \underset{n\to+\infty}{\sim} \frac{\pi}{2}$. Et donc $I_n^2 \underset{n\to+\infty}{\sim} \frac{\pi}{2n}$ puisque l'on peut diviser dans les relations d'équivalences. Et comme on peut élever aussi à une puissance réelle avec des suites à termes strictement positifs (et c'est le cas), on obtient donc

$$I_n \underset{n\to+\infty}{\sim} \sqrt{\frac{\pi}{2n}}$$

13. La suite (I_{2n}) est une sous-suite de la suite (I_n) et on a un équivalent de la suite (I_n). On en déduit donc un équivalent de la suite (I_{2n}) :

$$I_{2n} \underset{n\to+\infty}{\sim} \sqrt{\frac{\pi}{4n}} = \frac{1}{2}\sqrt{\frac{\pi}{n}}$$

Or $\forall n \in \mathbb{N}$, $I_{2n} = \frac{\pi}{2}\frac{(2n)!}{(2^n n!)^2}$ d'après la question 10. Et à la fin de la partie I dans la question 7, on a montré que

$$n! \underset{n\to+\infty}{\sim} C\sqrt{n}\left(\frac{n}{e}\right)^n$$

On en déduit donc

$$\begin{aligned} I_{2n} &\underset{n\to+\infty}{\sim} \frac{\pi}{2}\frac{C\sqrt{2n}\left(\frac{2n}{e}\right)^{2n}}{2^{2n}\left(C\sqrt{n}\left(\frac{n}{e}\right)^n\right)^2} \\ &= \frac{\pi}{2}\frac{C\sqrt{2n}(2n)^{2n}e^{2n}}{2^{2n}C^2nn^{2n}e^{2n}} \\ &= \frac{\pi}{C\sqrt{2n}} \end{aligned}$$

Par transitivité de la relation d'équivalence, on a donc

$$\frac{1}{2}\sqrt{\frac{\pi}{n}} \underset{n\to+\infty}{\sim} \frac{\pi}{C\sqrt{2n}}$$

Ce qui nous amène facilement à

$$C \underset{n\to+\infty}{\sim} \frac{\pi}{\sqrt{2}}\frac{2}{\sqrt{\pi}} = \sqrt{2\pi}$$

Mais comme les deux côtés sont des constantes, en passant à la limite et en utilisant l'unicité de la limite (par exemple), on a

$$C = \sqrt{2\pi}$$

Et on a fini (à 3 question près) la démo de l'équivalent de Stirling ! !

14. Application :

$$\begin{aligned} \alpha_n &= \frac{n!}{n^n} \\ &\underset{n\to+\infty}{\sim} \frac{1}{n^n}(n/e)^n\sqrt{2\pi n} \\ &\underset{n\to+\infty}{\sim} \frac{\sqrt{2\pi n}}{e^n} \xrightarrow[n\to+\infty]{} 0 \end{aligned}$$

par croissance comparée. Et

$$\begin{aligned} \beta_n &= \frac{(n!)}{n^n} \\ &\underset{n\to+\infty}{\sim} \frac{1}{n^n}(n/e)^{2n}(2\pi n) \\ &\underset{n\to+\infty}{\sim} (2\pi n)(n/e^2)^n \xrightarrow[n\to+\infty]{} +\infty \end{aligned}$$

Problème 2 (Deux groupes isomorphes) :

1. **Un produit semi-direct**

Soit $G = \mathbb{R}^* \times \mathbb{R}$. On pose

$$\forall (x,y),(x',y') \in G,\ (x,y)*(x',y') = (xx', y + xy').$$

(a) Soit $(x,y),(x',y') \in G$. Alors, $x, x' \in \mathbb{R}^*$. Et donc $xx' \in \mathbb{R}^*$ puisque $(\mathbb{R}^*, \times)$ est un groupe. De plus, $(\mathbb{R}, +, \times)$ un anneau, donc $y + xy' \in \mathbb{R}$. Et donc $(xx', y+xy') \in \mathbb{R}^* \times \mathbb{R} = G$. Donc $(x,y)*(x',y') \in G$. Donc $*$ est une LCI sur G.

Soit $(a,b) \in G$. On résout

$$\begin{aligned} \forall (x,y) \in G,\ (a,b)*(x,y) = (x,y) &\iff \forall (x,y) \in G,\ (ax, b+ay) = (x,y) \\ &\implies (a,b) = (1,0) && x=1,\ y=0 \end{aligned}$$

Puis on vérifie :

$$\forall (x,y) \in G,\ \begin{cases} (x,y)*(1,0) = (x, y + x\times 0) = (x,y) \\ (1,0)*(x,y) = (x, 0 + 1 \times y) = (x,y) \end{cases}$$

Donc, par définition, $(1,0)$ est élément neutre de $*$.

(b) $*$ est une LCI avec élément neutre sur G. Il reste à montrer qu'elle est associative et que tout élément de G est inversible pour $*$. On ne peut pas utiliser la caractérisation des sous-groupes car la loi utilisé n'est pas la loi naturel sur $\mathbb{R}$. Ce n'est donc pas un groupe produit.

Soit $(a,b),(c,d),(e,f) \in G$. Alors

$$\begin{aligned} ((a,b)*(c,d))*(e,f) &= (ac, b+ad)*(e,f) && \text{def } * \\ &= ((ac)e, (b+ad)+(ac)f) && \text{def } * \\ &= (ace, b+ad+acf) && \text{asso } + \text{ dans } \mathbb{R} \\ &= (ace, b + a(d+cf)) && \text{distributivité de } \times \text{ sur } + \\ &= (a,b)*(ce, d+cf) && \text{def } * \\ &= (a,b)*((c,d)*(e,f)) && \text{def } * \end{aligned}$$

Donc $*$ est associative.

De plus, si $(x,y) \in G$, alors

$$(x,y)*(\frac{1}{x}, -\frac{y}{x}) = (x \times \frac{1}{x}, y + x \times (-\frac{y}{x})) = (1,0)$$

Et

$$(\frac{1}{x}, -\frac{y}{x})*(x,y) = (\frac{1}{x}\times x, -\frac{y}{x} + \frac{1}{x} * y) = (1,0)$$

Or $(1,0)$ est élément neutre de $*$. Donc, par définition, $(x,y) \in G$ est inversible et $(x,y)^{-1} = (\frac{1}{x}, -\frac{y}{x})$.

Donc $(G,*)$ est un groupe ($*$ est une LCI sur G, associative, avec un élément neutre et pour lequel tout élément est inversible).

En revanche,

$$(2,1)*(1,2) = (2, 1+4) = (2,5) \quad \text{et} \quad (1,2)*(2,1) = (2, 2+1) = (2,3)$$

Donc $(2,1)*(1,2) \neq (1,2)*(2,1)$ et donc $*$ n'est pas commutative.

(c) Soit $H = \mathbb{R}^* \times \{0\}$ et $K = \{1\} \times \mathbb{R}$. Alors, par définition, $H, K \subset \mathbb{R}^* \times \mathbb{R} = G$.

De plus, $(1,0) \in H$. Soit $h, h' \in H$. Donc $\exists x, x' \in \mathbb{R}^*$ tel que $h = (x,0)$ et $h' = (x', 0)$. Alors

$$\begin{aligned} h * h'^{-1} &= (x,0)*(x',0)^{-1} \\ &= (x,0)*(1/x', 0) && \text{def inverse pour } * \\ &= \left(x \times \frac{1}{x'}, 0\right) && \text{def } * \end{aligned}$$

$$= \left(\frac{x}{x'}, 0\right) \in H$$

Donc, par caractérisation des sou-groupes, H est un sous-groupe de G.

De même, $(1,0) \in \{1\} \times \mathbb{R} = K$. Soit $k, k' \in K$. Donc $\exists y, y' \in \mathbb{R}$ tel que $k = (1, y)$ et $k' = (1, y')$. Alors

$$\begin{aligned}
k * k'^{-1} &= (1, y) * (1, y')^{-1} \\
&= (1, y) * \left(\frac{1}{1}, -\frac{y'}{1}\right) && \text{def inverse pour } * \\
&= (1, y) * (1, -y') \\
&= (1, y - y') \in K.
\end{aligned}$$

Donc, par caractérisation des sou-groupes, K est un sous-groupe de $(G, *)$.

2. **Les transformations affines de $\mathbb{R}$**

On note $\mathcal{S}(\mathbb{R})$ les bijections de $\mathbb{R}$ dans $\mathbb{R}$.

(a) $\mathrm{Id}_{\mathbb{R}} \in \mathcal{S}(\mathbb{R})$. Et par définition de $\mathrm{Id}_{\mathbb{R}}$, $\forall f \in \mathcal{S}(\mathbb{R})$, $f \circ \mathrm{Id}_{\mathbb{R}} = \mathrm{Id}_{\mathbb{R}} \circ f = f$. Donc $\mathrm{Id}_{\mathbb{R}}$ est un élément neutre pour $\circ$.

On sait déjà que $\circ$ est associative dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$. Donc $\circ$ est associative sur $\mathcal{S}(\mathbb{R})$ car $\mathcal{S}(\mathbb{R}) \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$.

Par ailleurs, on sait aussi que $\circ$ est une LCI sur $\mathcal{S}(\mathbb{R})$ (la composée de deux bijections est une bijection).

Par définition de $\mathcal{S}(\mathbb{R})$ et par caractérisation de la bijectivité, toute fonction de $\mathcal{S}(\mathbb{R})$ est inversible pour $\circ$ ($\forall f \in \mathcal{S}(\mathbb{R})$, f est bijective, donc $\forall f \in \mathcal{S}(\mathbb{R})$, $\exists g \in \mathcal{S}(\mathbb{R})$, $f \circ g = g \circ f = \mathrm{Id}_{\mathbb{R}}$).

Donc, par définition, $(\mathcal{S}(\mathbb{R}), \circ)$ est une groupe.

(b) Par définition, $\mathrm{Aff}(\mathbb{R}) \subset \mathcal{S}(\mathbb{R})$.

Clairement, $\forall x, y \in \mathbb{R}$, $\forall t \in \mathbb{R}$, $\mathrm{Id}_{\mathbb{R}}(tx + (1-t)y) = tx + (1-t)y = t\,\mathrm{Id}_{\mathbb{R}}(x) + (1-t)\,\mathrm{Id}_{\mathbb{R}}(y)$. Donc $\mathrm{Id}_{\mathbb{R}} \in \mathrm{Aff}(\mathbb{R})$.

Soit $f, g \in \mathrm{Aff}(\mathbb{R})$. Alors

$$\begin{aligned}
\forall x, y, t \in \mathbb{R},\ (f \circ g)(tx + (1-t)y) &= f(g(tx + (1-ty))) && \text{def } \circ \\
&= f(tg(x) + (1-t)g(y)) && \text{car } g \in \mathrm{Aff}(\mathbb{R}) \\
&= tf(g(x)) + (1-t)f(g(y)) && \text{car } f \in \mathrm{Aff}(\mathbb{R}) \\
&= t(f \circ g)(x) + (1-t)(f \circ g)(y) && \text{def } \circ
\end{aligned}$$

Donc, par définition de $\mathrm{Aff}(\mathbb{R})$, $f \circ g \in \mathrm{Aff}(\mathbb{R})$.

Soit $f \in \mathrm{Aff}(\mathbb{R})$. Soit $x, y, t \in \mathbb{R}$. f est bijection donc $\exists a, b \in \mathbb{R}$ tel que $x = f(a)$ et $y = f(b)$. Et donc

$$\begin{aligned}
f^{-1}(tx + (1-t)y) &= f^{-1}(tf(a) + (1-t)f(b)) && \text{def } a, b \\
&= f^{-1}(f(ta + (1-t)b)) && \text{car } f \in \mathrm{Aff}(\mathbb{R}) \\
&= ta + (1-t)b \\
&= tf^{-1}(x) + (1-t)f^{-1}(y).
\end{aligned}$$

Donc $f^{-1} \in \mathrm{Aff}(\mathbb{R})$.

Donc, par caractérisation des sous-groupes, $\mathrm{Aff}(\mathbb{R})$ est un sous-groupe de $(\mathcal{S}(\mathbb{R}), \circ)$.

3. **Un isomorphisme**

On note $\forall a, b \in \mathbb{R}$, $f_{a,b} : x \mapsto ax + b$.

(a) Soit $a, b \in \mathbb{R}$. Alors

$$\begin{aligned}
\forall x, y, t \in \mathbb{R},\ f_{a,b}(tx + (1-t)y) &= a(tx + (1-t)y) + b && \text{def } f_{a,b} \\
&= atx + (1-t)ay + (t + (1-t))b \\
&= t(ax + b) + (1-t)(ay + b) && (\mathbb{R}, +, \times) \text{ anneau commutatif} \\
&= tf_{a,b}(x) + (1-t)f_{a,b}(y) && \text{def } f_{a,b}
\end{aligned}$$

Donc $f_{a,b}$ est affine.

Il et facile de vérifier que $f_{a,b}$ est bijective si, et seulement si, $a \neq 0$. En effet, si $a \neq 0$, alors

$$\begin{aligned} \forall x \in \mathbb{R},\ f_{a,b} \circ f_{\frac{1}{a},-\frac{b}{a}}(x) &= f_{a,b}(x/a - b/a) \\ &= a(x/a - b/a) + b \\ &= x \end{aligned} \qquad \begin{aligned} f_{1/a,-b/a} \circ f_{a,b}(x) &= f_{a,b}(x)/a - b/a \\ &= (ax+b)/a - b/a \\ &= x \end{aligned}$$

Donc $f_{a,b} \circ f_{1/a,-b/a} = f_{1/a,-b/a} \circ f_{a,b} = \mathrm{Id}_{\mathbb{R}}$. Et $f_{0,b}$ est une fonction constante, donc en particulier non injective, donc non bijective. Donc $f_{a,b}$ inversible si, et seulement si, $a \neq 0$.

(b) Soit

$$F : \begin{array}{ccc} G & \to & \mathrm{Aff}(\mathbb{R}) \\ (a,b) & \mapsto & f_{a,b} \end{array}$$

Alors

$$\begin{aligned} \forall (a,b),(c,d) \in G,\ \forall x \in \mathbb{R},\ F((a,b) * (c,d))(x) &= F((ac, b+ad))(x) && \text{def } * \\ &= f_{ac,b+ad}(x) && \text{def } F \\ &= acx + b + ad && \text{def } f_{ac,b+ad} \\ &= a(cx+d) + b && (\mathbb{R},+,\times) \text{ anneau} \\ &= af_{c,d}(x) + b && \text{def } f_{c,d} \\ &= f_{a,b}(f_{c,d}(x)) && \text{def } f_{a,b} \\ &= (f_{a,b} \circ f_{c,d})(x) && \text{def } \circ \\ &= (F(a,b) \circ F(c,d))(x) && \text{def } F \end{aligned}$$

Donc, par définition de l'égalité entre applications, $\forall (a,b),(c,d) \in G,\ F((a,b) * (c,d)) = F(a,b) \circ F(c,d)$.

Donc $F : (G, *) \to (\mathrm{Aff}(\mathbb{R}), \circ)$ est un morphisme de groupe.

(c) On pose

$$\varphi : \begin{array}{ccc} \mathrm{Aff}(\mathbb{R}) & \to & G \\ f & \mapsto & (f(1) - f(0), f(0)) \end{array}$$

Vérifions d'abord que cette application est bien définie. Soit $f \in \mathrm{Aff}(\mathbb{R})$. Alors f est bijective, par définition de $\mathrm{Aff}(\mathbb{R})$. En particulier, f est injective. Or $1 \neq 0$, donc $f(1) \neq f(0)$. Donc $f(1) - f(0) \in \mathbb{R}^*$. Donc $\varphi(f) \in \mathbb{R}^* \times \mathbb{R} = G$. Donc φ est bien définie.

Soit $g \in \mathrm{Aff}(\mathbb{R})$ et $x \in \mathbb{R}$. Alors $x = x \times 1 + (1-x) \times 0$. Donc, par définition de $\mathrm{Aff}(\mathbb{R})$,

$$g(x) = g(x \times 1 + (1-x) \times 0) = xg(1) + (1-x)g(0) = (g(1) - g(0)x + g(0) = f_{g(1)-g(0),g(0)}(x).$$

Donc, par définition de l'égalité entre applications, $g = f_{g(1)-g(0),g(0)}$. Autrement dit

$$\forall g \in \mathrm{Aff}(\mathbb{R}),\ F \circ \varphi(g) = F(g(1) - g(0), g(0)) = f_{g(1)-g(0),g(0)} = g.$$

donc $F \circ \varphi = \mathrm{Id}_{\mathrm{Aff}(\mathbb{R})}$.

Et

$$\forall (a,b) \in G,\ \varphi \circ F(a,b) = \varphi(f_{a,b}) = (f_{a,b}(1) - f_{a,b}(0), f_{a,b}(0)) = (a+b-b, b) = (a,b).$$

Donc $\varphi \circ F = \mathrm{Id}_G$.

Donc par caractérisation de la bijectivité, F est bijective et $F^{-1} = \varphi$.

Or F est morphisme de groupes. Donc $F : (G, *) \to (\mathrm{Aff}(\mathbb{R}), \circ)$ est un isomorphisme de groupes.

Supposons $(\mathrm{Aff}(\mathbb{R}), \circ)$ abélien. Soit $(a,b),(c,d) \in G$. Soit $f = F(a,b)$ et $g = F(c,d)$. Donc $(a,b) = F^{-1}(f) = \varphi(f)$ et $(c,d) = F^{-1}(g) = \varphi(g)$. Alors

$$\begin{aligned} (a,b) * (c,d) &= F^{-1}(f) * F^{-1}(g) && F \text{ bijective} \\ &= F^{-1}(f \circ g) && \text{car } F \text{ morphisme} \end{aligned}$$

$$\begin{aligned} &= F^{-1}(g \circ f) && \text{Aff}(\mathbb{R}) \text{ abélien par hypothèse} \\ &= F^{-1}(g) * F^{-1}(f) && F \text{ morphisme} \\ &= (c,d) * (a,b) \end{aligned}$$

Donc G abélien. Or G n'est pas abélien d'après la question 1b. On a donc une contradiction. Donc $(\text{Aff}(\mathbb{R}), \circ)$ n'est pas abélien.

4. **Les automorphismes intérieurs de G**

(a) Soit $g \in G$ et $\varphi_g : G \to G$ définie par $\forall h \in G$, $\varphi_g(h) = g * h * g^{-1}$.

Alors

$$\begin{aligned} \forall h, h' \in G,\ \varphi_g(h * h') &= g * (h * h') * g^{-1} && \text{def } \varphi_g \\ &= g * h * (1,0) * h' * g^{-1} && \text{associativité et neutre de } G \\ &= g * h * (g^{-1} * g) * h' * g^{-1} && \text{neutre de } G \\ &= (g * h * g^{-1}) * (g * h' * g^{-1}) && \text{associativité} \\ &= \varphi_g(h) * \varphi_g(h') && \text{def } \varphi_g \end{aligned}$$

Donc, par définition, φ_g est un morphisme de groupes.

Puis

$$\begin{aligned} \forall h \in G,\ (\varphi_g \circ \varphi_{g^{-1}})(h) &= g * (\varphi_{g^{-1}}(h)) * g^{-1} && \text{def } \varphi_g \\ &= g * (g^{-1} * h * (g^{-1})^{-1}) * g^{-1} && \text{def } \varphi_{g^{-1}} \\ &= (g * g^{-1}) * h * (g * g^{-1}) && \text{associativité et involution du passage à l'inverse} \\ &= h \end{aligned}$$

Donc $\varphi_g \circ \varphi_{g^{-1}} = \text{Id}_G$.

De même,

$$\begin{aligned} \forall h \in G,\ \varphi_{g^{-1}} \circ \varphi_g(h) &= g^{-1} * \varphi_g(h) * (g^{-1})^{-1} && \text{def } \varphi_{g^{-1}} \\ &= g^{-1} * (g * h * g^{-1}) * g && \text{def } \varphi_g \text{ et involution du passage à l'inverse} \\ &= (g^{-1} * g) * h * (g^{-1} * g) && \text{associativité} \\ &= h \end{aligned}$$

Donc $\varphi_{g^{-1}} \circ \varphi_g = \text{Id}_G$.

Donc, par caractérisation de la bijectivité, φ_g est bijective et $\varphi_g^{-1} = \varphi_{g^{-1}}$.

(b) Soit $a \in \mathbb{R}$. Donc $(1,a) \in \{1\} \times \mathbb{R} = K$. Soit $g = (x,y) \in G$. Alors

$$\begin{aligned} \varphi_g((1,a)) &= g * (1,a) * g^{-1} && \text{def } \varphi_g \\ &= (x,y) * (1,a) * (1/x, -y/x) && \text{cf } 1b \\ &= (x,y) * (1/x, a - ay/x) && \text{def } * \\ &= (x/x, y + x(a - ay/x)) && \text{def } * \\ &= (1, y + xa - ay) \end{aligned}$$

Donc $\forall g \in G$, $\forall (1,a) \in K$, $\varphi_g((1,a)) \in K$. Donc $\forall g \in G$, $\varphi_g(K) \subset K$. Donc K est stable par φ_g.

Soit $a \in R^*$. Alors $(a,0) \in H = \mathbb{R}^* \times \{0\}$. Soit $(x,y) \in G$. Alors

$$\begin{aligned} \varphi_{(x,y)}((a,0)) &= (x,y) * (a,0) * (x,y)^{-1} && \text{def } \varphi_{(x,y)} \\ &= (xa, y) * (1/x, -y/x) && \text{def } * \text{ et inverse} \\ &= (a, y - ya) \end{aligned}$$

En particulier, si $y \neq 0$ et $a \neq 1$, alors $\forall x \in \mathbb{R}^*$, $\varphi_{(x,y)}((a,0)) = (a, y(1-a)) \notin \mathbb{R}^* \times \{0\} = H$. Plus précisément, $\varphi_{(1,2)}(2,0) = (2,-2) \notin H$. Donc H n'est pas toujours stable par les automorphismes intérieurs. Autrement dit, $\exists g \in G$ tel que $\varphi_g(H) \not\subset H$.

On note $\forall g \in G$, $\widetilde{\varphi_g} : K \to K$ l'endomorphisme de K induit par φ_g (puisque K est stable par φ_g).

(c) Soit

$$\Phi : \begin{array}{ccc} H & \to & \mathrm{Aut}(K) \\ h & \mapsto & \widetilde{\varphi_h} \end{array}$$

Tout d'abord, $\forall g \in G$, K est stable par φ_g. Donc $\forall g \in G$, $\widetilde{\varphi_g}$ est bien définie. De plus, $\forall g \in G$, φ_g est un morphisme de groupe. Donc $\forall g \in G$, $\widetilde{\varphi_g}$ est un morphisme de groupe. Donc $\forall g \in G$, $\widetilde{\varphi_g}$ est un endomorphisme de K. De plus, $\forall g \in G$, φ_g est bijective (cf 4a). Donc $\forall g \in G$, $\widetilde{\varphi_g}$ est bijective. Donc $\forall g \in G$, $\widetilde{\varphi_g}$ est un automorphisme de K. Donc $\forall g \in G$, $\widetilde{\varphi_g} \in \mathrm{Aut}(K)$. Donc Φ est bien définie.

Commençons par un petit calcul préalable général :

$$\begin{aligned} \forall g,h \in G,\ \forall x \in G,\ \varphi_g \circ \varphi_h(x) &= g * (h * x * h^{-1}) * g^{-1} && \text{def } \circ,\ \varphi_g, \varphi_h \\ &= (g * h) * x * (g * h)^{-1} && \text{associativité et inverse d'un produit} \\ &= \varphi_{g*h}(x). \end{aligned}$$

Donc, par égalité entre applications, $\forall g, h \in G$, $\varphi_g \circ \varphi_h = \varphi_{g*h}$.

Soit $h, h' \in H$. Alors

$$\begin{aligned} \Phi(h * h') &= \widetilde{\varphi_{h*h'}} && \text{def } \Phi \\ &= \widetilde{\varphi_h \circ \varphi_{h'}} && \text{cf au-dessus} \\ &= \widetilde{\varphi_h} \circ \widetilde{\varphi_{h'}} \\ &= \Phi(h) \circ \Phi(h') \end{aligned}$$

Donc Φ est un morphisme de groupe.

(d) Soit $h \in H$. Donc $\exists a \in \mathbb{R}*$ tel que $h = (a, 0)$ par définition de H. Étudions le noyau de Φ.

$$\begin{aligned} h \in \ker(\Phi) &\iff \Phi(h) = \mathrm{Id}_K && \text{def } \ker(\Phi) \\ &\iff \widetilde{\varphi_h} = \mathrm{Id}_K && \text{def } \Phi \\ &\iff \forall k \in K,\ \widetilde{\varphi_h}(k) = k && \text{def égalité entre applications} \\ &\iff \forall k \in K,\ h * k * h^{-1} = k && \text{def } \widetilde{\varphi_h} \\ &\iff \forall k \in K,\ h * k = k * h \\ &\iff \forall x \in \mathbb{R},\ (a,0) * (1,x) = (1,x) * (a,0) && \text{def } K \\ &\iff \forall x \in \mathbb{R},\ (a, ax) = (a, x) && \text{def } * \\ &\iff \forall x \in \mathbb{R},\ ax = x && \text{égalité dans un produit cartésien} \\ &\iff a = 1 && \text{prendre } x = 1 \iff h = (1,0) \quad \text{def } h \end{aligned}$$

D'où $\ker(\Phi) = \{(1,0)\}$. Or $(1,0)$ est l'élément neutre de G, donc de H. Donc, par caractérisation de l'injectivité par le noyau, Φ est injective.