

Questions de cours

1. A est intègre s'il est non nul et si $\forall x, y \in A, xy = 0_A \Rightarrow [x = 0_A \text{ ou } y = 0_A]$.
2. K est un corps si c'est un anneau commutatif dans lequel tout élément non nul possède un inverse pour la loi \times .
3. Soit I intervalle de \mathbb{R} , soit $a \in I$, soit $f \in \mathcal{C}^k(I \setminus \{a\}, \mathbb{R})$. On suppose que pour tout $j \in \llbracket 0, k \rrbracket$, $\lim_{x \rightarrow a} f^{(j)}(x)$ existe dans \mathbb{R} . Alors f admet un prolongement de classe \mathcal{C}^k à I entier et pour tout $j \in \llbracket 0, k \rrbracket$, $f^{(j)}(a) = \lim_{x \rightarrow a} f^{(j)}(x)$.

Problème 1 : approximation d'une fonction réciproque

I. Étude de f et g

1. La fonction f est strictement croissante sur \mathbb{R} comme somme de deux fonctions croissantes sur \mathbb{R} . De plus, f est impaire : on peut donc limiter l'étude à \mathbb{R}_+ . On a $f(0) = 0$, de plus f est dérivable sur \mathbb{R} et pour tout $x \in \mathbb{R}$, $f'(x) = 3x^2 + 1$. Ainsi $f'(0) = 1$ et la droite d'équation $y = x$ est tangente au graphe de f en O . Comme pour $x \in \mathbb{R}_+$, on a $x^3 \geq 0$, alors $f(x) = x^3 + x \geq x$ et le graphe de f est situé au-dessus de la tangente en O sur \mathbb{R}_+ . Enfin, $\lim_{x \rightarrow +\infty} f(x) = +\infty$.
On trace alors le graphe de f sur \mathbb{R}_+ puis on en déduit le graphe sur \mathbb{R}_- par une symétrie de centre O .

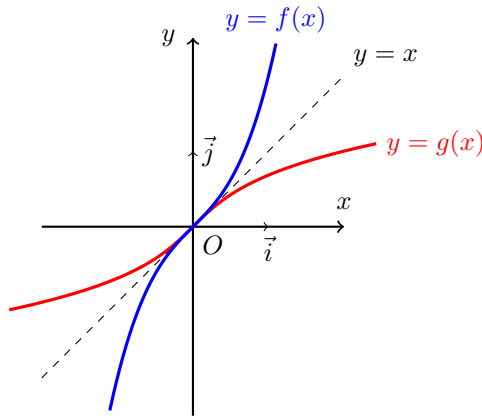


FIGURE 1 – Graphes de f et g

2. La fonction f est continue et strictement croissante. D'après le théorème de la bijection monotone, elle réalise donc une bijection de \mathbb{R} sur son image. Et comme $\lim_{x \rightarrow -\infty} f(x) = -\infty$ et $\lim_{x \rightarrow +\infty} f(x) = +\infty$, f réalise une bijection de \mathbb{R} sur \mathbb{R} .

3. La fonction g est la réciproque d'une fonction strictement croissante et impaire : elle est donc strictement croissante et impaire. On déduit son graphe de celui de f par symétrie par rapport à la droite d'équation $y = x$.
4. On a, pour tout $x \in \mathbb{R}$, $f'(x) = 3x^2 + 1 \neq 0$. Par conséquent g est dérivable sur \mathbb{R} et pour tout $x \in \mathbb{R}$, $g'(x) = \frac{1}{f'(g(x))} = \frac{1}{3g(x)^2 + 1}$.
La fonction g étant impaire, la fonction $x \mapsto g(x)^2$ est paire et donc g' est paire. La fonction g et la fonction $x \mapsto x^2$ étant croissantes sur \mathbb{R}_+ , la fonction $x \mapsto 3g(x)^2 + 1$ est croissante et strictement positive sur \mathbb{R}_+ . Par conséquent g' est décroissante sur \mathbb{R}_+ , et donc croissante sur \mathbb{R}_- par parité.
5. D'après ce qui précède, la fonction g est convexe sur \mathbb{R}_- et concave sur \mathbb{R}_+ . Par conséquent elle présente un unique point d'inflexion en O .

II. Approximation de g par la méthode de Newton

6. Soit $x \in \mathbb{R}_+$.
Notons (a, b) les coordonnées du point d'intersection entre D_t et la tangente à \mathcal{C}_f en $(x, f(x))$. On a $b = t$ et $b = f'(x)(a - x) + f(x) = (3x^2 + 1)(a - x) + x^3 + x$ d'où $a = x + \frac{t - x^3 - x}{3x^2 + 1} = \frac{3x^3 + x + t - x^3 - x}{3x^2 + 1} = \frac{2x^3 + t}{3x^2 + 1} = \varphi_t(x)$.
En particulier, pour tout $n \in \mathbb{N}$, en prenant $x = u_n$, on a $u_{n+1} = \varphi_t(u_n)$.
7. (a) On calcule : $\varphi_t(x) - x = \frac{2x^3 + t}{3x^2 + 1} - x = \frac{t - x^3 - x}{3x^2 + 1} = \frac{t - f(x)}{3x^2 + 1}$.
Donc $\varphi_t(x) - x \geq 0 \Leftrightarrow f(x) \leq t \Leftrightarrow x \leq g(t)$ en appliquant la fonction g qui est croissante. Et on a $\varphi_t(x) = x \Leftrightarrow f(x) = t \Leftrightarrow x = g(t)$.
- (b) La fonction φ_t est le quotient de deux fonctions dérivables, celle du dénominateur n'étant jamais nulle. Par conséquent, φ_t est dérivable sur \mathbb{R} et $\varphi_t'(x) = \frac{6x^2(3x^2 + 1) - 6x(2x^3 + t)}{(3x^2 + 1)^2} = \frac{6x(x^3 + x - t)}{(3x^2 + 1)^2} = \frac{6x(f(x) - t)}{(3x^2 + 1)^2}$.
Or $f(x) \geq t \Leftrightarrow x \geq g(t)$ par croissance de la fonction g .
On en déduit le tableau de signe suivant :

x	$-\infty$	0	$g(t)$	$+\infty$
$6x$		-	0	+
$f(x) - t$		-	-	0
$(3x^2 + 1)^2$		+	+	+
$\varphi_t'(x)$		+	0	-

- (c) On a $g(t) \leq t \Leftrightarrow t \leq f(t) = t^3 + t$ par croissance de f , et cette dernière inégalité est vraie puisque $t \in \mathbb{R}_+$. Donc $g(t) \leq t$.
D'après ce qui précède, φ_t est croissante sur $[g(t), t]$.
En outre, $\varphi_t(g(t)) - g(t) = \frac{t - f(g(t))}{3g(t)^2 + 1} = \frac{t - t}{3g(t)^2 + 1} = 0$ d'après le calcul

effectué à la question 7a. Donc $\varphi(g(t)) = t$. Et comme $t \geq g(t)$, toujours d'après la question 7a, $\varphi_t(t) - t \leq 0$ donc $\varphi_t(t) \leq t$.

Ainsi, pour tout $u \in [g(t), t]$, on a $g(t) \leq \varphi_t(u) \leq \varphi_t(t) \leq t$, et l'intervalle $[g(t), t]$ est stable par φ_t .

- (d) Soit $x \in [g(t), t]$. Comme $x \leq t$, on a $x - t \leq 0$ d'où $x^3 + x - t \leq x^3$. Et comme $x \geq g(t)$, on a $f(x) \geq t$ soit $x^3 + x \geq t$ et $x^3 + x - t \geq 0$.

Et comme $g(t) \geq 0$, on a aussi $x \geq 0$ et il s'ensuit

$$0 \leq \varphi'_t(x) = \frac{6x(x^3 + x - t)}{(3x^2 + 1)^2} \leq \frac{6x}{(3x^2 + 1)^2} x^3 = \frac{6x^4}{9x^4 + 6x^2 + 1} \leq \frac{6x^4}{9x^4} = \frac{2}{3}$$

autrement dit, $0 \leq \varphi'_t(x) \leq \frac{2}{3}$.

8. (a) On a $u_0 = t \in [g(t), t]$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = \varphi_t(u_n)$ d'après la question 6. Comme l'intervalle $[g(t), t]$ est stable par φ_t d'après la question 7c, on en déduit que pour tout $n \in \mathbb{N}$, $u_n \in [g(t), t]$.

- (b) Pour tout $n \in \mathbb{N}$, $u_{n+1} - u_n = \varphi_t(u_n) - u_n \leq 0$ d'après la question 7a puisque $u_n \geq g(t)$. Donc $(u_n)_{n \in \mathbb{N}}$ est décroissante, et minorée par $g(t)$. D'après le théorème de la limite monotone, elle converge. Et comme φ_t est continue, la limite de $(u_n)_{n \in \mathbb{N}}$ est un point fixe de φ_t , donc $g(t)$ d'après la question 7a.

- (c) D'après la question 7d, on a pour tout $s \in [g(t), t]$, $|\varphi'_t(s)| \leq \frac{2}{3}$. La fonction φ_t est par conséquent $\frac{2}{3}$ -lipschitzienne sur $[g(t), t]$ d'après l'inégalité des accroissements finis.

Alors, pour tout $n \in \mathbb{N}$, $u_n \geq g(t)$ d'où $|u_n - g(t)| = u_n - g(t)$, et

$$0 \leq u_{n+1} - g(t) = |\varphi_t(u_n) - \varphi_t(g(t))| \leq \frac{2}{3}(u_n - g(t))$$

- (d) Soit $t \in [0, a]$.

On déduit par récurrence de la question précédente que pour tout $n \in \mathbb{N}$,

$$u_n - g(t) \leq \left(\frac{2}{3}\right)^n (u_0 - g(t)) = \left(\frac{2}{3}\right)^n (t - g(t))$$

Or comme $0 \leq g(t) \leq t \leq a$, on a $0 \leq t - g(t) \leq a$ d'où

$$u_n - g(t) \leq \left(\frac{2}{3}\right)^n a$$

Par suite, $\beta_n = \sup_{t \in [0, a]} (u_n - g(t)) \leq \left(\frac{2}{3}\right)^n a$.

- (e) Soit $x \in \mathbb{R}_+$. Calculons

$$\begin{aligned} (x - g(t))^2(2x + g(t)) &= (x^2 - 2xg(t) + g(t)^2)(2x + g(t)) \\ &= 2x^3 + x^2g(t) - 4x^2g(t) - 2xg(t)^2 + 2xg(t)^2 + g(t)^3 \\ (x - g(t))^2(2x + g(t)) &= 2x^3 - 3x^2g(t) + g(t)^3 \end{aligned}$$

Mais comme g est la réciproque de f , on a $g(t)^3 + g(t) = t$.

Par conséquent $g(t)^3 = t - g(t)$ et

$$(x - g(t))^2 \frac{2x + g(t)}{3x^2 + 1} = \frac{2x^3 - 3x^2g(t) + t - g(t)}{3x^2 + 1} = \frac{2x^3 + t}{3x^2 + 1} - g(t) \frac{3x^2 + 1}{3x^2 + 1}$$

ce qui permet de conclure que $(x - g(t))^2 \frac{2x + g(t)}{3x^2 + 1} = \varphi_t(x) - g(t)$.

- (f) Soit $x \in [g(t), t]$. On a alors $\frac{2x + g(t)}{3x^2 + 1} \leq \frac{3x}{3x^2 + 1}$.

Étudions les variations de la fonction $h : x \mapsto \frac{3x}{3x^2 + 1}$.

Cette fonction est définie et dérivable sur \mathbb{R}_+ , et pour tout $x \in \mathbb{R}_+$,

$$h'(x) = \frac{3(3x^2 + 1) - 3x \times 6x}{(3x^2 + 1)^2} = \frac{3(1 - 3x^2)}{(3x^2 + 1)^2}$$

Le dénominateur étant toujours positif, ce quotient est du même signe que $1 - 3x^2$, donc positif sur $[0, \frac{1}{\sqrt{3}}]$ et négatif sur $[\frac{1}{\sqrt{3}}, +\infty[$.

Par conséquent h est croissante sur $[0, \frac{1}{\sqrt{3}}[$ et décroissante sur $]\frac{1}{\sqrt{3}}, +\infty[$. Elle possède par conséquent un maximum en $\frac{1}{\sqrt{3}}$.

Celui-ci vaut $h\left(\frac{1}{\sqrt{3}}\right) = \frac{\frac{3}{\sqrt{3}}}{\frac{3}{3} + 1} = \frac{\sqrt{3}}{2}$. Ainsi pour tout $x \in \mathbb{R}_+$, $h(x) \leq \frac{\sqrt{3}}{2}$.

Par conséquent, pour tout $x \in [g(t), t]$,

$$0 \leq \varphi_t(x) - g(t) = (x - g(t))^2 \frac{2x + g(t)}{3x^2 + 1} \leq h(x)(x - g(t))^2 \leq \frac{\sqrt{3}}{2}(x - g(t))^2$$

Problème 2 - Étude du groupe $SL_2(\mathbb{Z})$

I. Déterminant et trace d'une matrice 2×2

1. Soient $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$.

On a alors $M + M' = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$ et $\text{tr}(M + M') = a + a' + d + d'$, mais $\text{tr}(M) + \text{tr}(M') = a + d + a' + d' = \text{tr}(M + M')$.

Soit $\lambda \in \mathbb{R}$. On a $\text{tr}(\lambda M) = \lambda a + \lambda d = \lambda(a + d) = \lambda \text{tr}(M)$.

2. On a $MM' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + c'd & b'c + dd' \end{pmatrix}$ et $M'M = \begin{pmatrix} aa' + b'c & a'b + b'd \\ ac' + cd' & bc' + dd' \end{pmatrix}$, d'où $\text{tr}(MM') = aa' + bc' + b'c + dd' = \text{tr}(M'M)$.

3. (a) D'après le calcul précédent,

$$\begin{aligned} \det(MM') &= (aa' + bc')(b'c + dd') - (a'c + c'd)(ab' + bd') \\ &= aa'b'c + aa'dd' + bb'cc' + bc'dd' - aa'b'c - a'bcd' - ab'c'd - bc'dd' \end{aligned}$$

$$\det(MM') = aa'dd' + bb'cc' - a'bcd' - ab'c'd$$

et $\det(M)\det(M') = (ad - bc)(a'd' - b'c') = aa'dd' + bb'cc' - a'bcd' - ab'c'd$ ce qui permet de conclure que $\det(MM') = \det(M)\det(M')$.

(b) Soit $M \in GL_2(\mathbb{R})$. On a $\det(M)\det(M^{-1}) = \det(MM^{-1}) = \det(I_2) = 1$ d'où $\det(M^{-1}) = \frac{1}{\det(M)}$.

(c) On a montré que \det réalise un morphisme de groupes de $(GL_2(\mathbb{R}), \times)$ dans (\mathbb{R}^*, \times) .

4. (a) Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$. On a $M^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & bc + d^2 \end{pmatrix}$ et

$$\begin{aligned} \text{tr}(M)M - \det(M)I_2 &= (a+d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \begin{pmatrix} a^2 + ad - ad + bc & b(a+d) - 0 \\ c(a+d) - 0 & ad + d^2 - ad + bc \end{pmatrix} \end{aligned}$$

$$\text{tr}(M)M - \det(M)I_2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & bc + d^2 \end{pmatrix} = M^2$$

ce qui prouve que $M^2 - \text{tr}(M)M + \det(M)I_2 = 0$.

(b) Comme M est inversible, on a $\det(M) \neq 0$.

On a alors $\frac{1}{\det(M)}(\text{tr}(M)M - M^2) = I_2$, ce qui se réécrit également

$$\frac{1}{\det(M)}(\text{tr}(M)I_2 - M)M = M \times \frac{1}{\det(M)}(\text{tr}(M)I_2 - M) = I_2.$$

Par conséquent, $M^{-1} = \frac{1}{\det(M)}(\text{tr}(M)I_2 - M)$.

II. Le groupe $SL_2(\mathbb{Z})$

5. Comme pour tout $M \in SL_2(\mathbb{Z})$, $\det(M) = 1 \neq 0$, on a $SL_2(\mathbb{Z}) \subset GL_2(\mathbb{R})$.

De plus, $I_2 \in \mathcal{M}_2(\mathbb{Z})$ et $\det(I_2) = 1$ donc $I_2 \in SL_2(\mathbb{Z})$ et $SL_2(\mathbb{Z}) \neq \emptyset$.

Soient $M, N \in SL_2(\mathbb{Z})$. Alors MN est à coefficients entiers relatifs, et $\det(MN) = \det(M)\det(N) = 1$ donc $MN \in SL_2(\mathbb{Z})$.

Par ailleurs, $M^{-1} = \frac{1}{\det(M)}(\text{tr}(M)I_2 - M) = \text{tr}(M)I_2 - M \in \mathcal{M}_2(\mathbb{Z})$ et

$$\det(M^{-1}) = \frac{1}{\det(M)} = 1 \text{ donc } M^{-1} \in SL_2(\mathbb{Z}).$$

Par conséquent, $SL_2(\mathbb{Z})$ est un sous-groupe de $GL_2(\mathbb{R})$.

6. On a clairement $S \in \mathcal{M}_2(\mathbb{Z})$, $T \in \mathcal{M}_2(\mathbb{Z})$, et

$$\det(S) = 0 \times 0 - 1 \times (-1) = 1 \quad \det(T) = 1 \times 1 - 0 \times 1 = 1$$

Par conséquent, S et T appartiennent à $SL_2(\mathbb{Z})$. La formule de l'inverse pour les

matrices 2×2 donne $S^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

7. On calcule $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$.

Donc $TS \neq ST$, les matrices S et T ne commutent pas.

8. Pour tout $k \in \mathbb{N}$, soit $\mathcal{P}(k)$ l'assertion « $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ et $T^{-k} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$ ».

Initialisation : on a $T^0 = I_2$ et $T^{-0} = I_2$, on a bien $\mathcal{P}(0)$ vraie.

Hérédité : soit $k \in \mathbb{N}$ tel que $\mathcal{P}(k)$ soit vraie. On calcule alors, avec l'hypothèse de récurrence,

$$T^{k+1} = T^k T = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$$

$$\text{et } T^{-(k+1)} = T^{-k} T^{-1} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(k+1) \\ 0 & 1 \end{pmatrix}$$

ce qui prouve que $\mathcal{P}(k+1)$ est vraie.

Ainsi, pour tout $k \in \mathbb{Z}$, $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.

9. On calcule $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$. Par conséquent, pour tout $n \in \mathbb{N}$,

$$S^{2n} = (-I_2)^n = (-1)^n I_2 \text{ et } S^{2n+1} = S^{2n} S = (-1)^n S.$$

Ainsi, pour tout $k \in \mathbb{Z}$, $S^k = \begin{cases} (-1)^{(k-1)/2} S & \text{si } k \text{ est impair} \\ (-1)^{k/2} I_2 & \text{si } k \text{ est pair} \end{cases}$.

10. Soit $M \in SL_2(\mathbb{Z})$.

(a) Supposons $\mu(M) = 0$. Alors $M = \begin{pmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{pmatrix}$ avec $m_{11}, m_{12}, m_{22} \in \mathbb{Z}$.

Mais $1 = \det(M) = m_{11}m_{22}$: donc $m_{11} = m_{22} = \pm 1$.

• Si $m_{11} = m_{22} = 1$, alors $M = \begin{pmatrix} 1 & m_{12} \\ 0 & 1 \end{pmatrix} = T^{m_{12}} \in \langle S, T \rangle$.

• Si $m_{11} = m_{22} = -1$, alors

$$M = \begin{pmatrix} -1 & m_{12} \\ 0 & -1 \end{pmatrix} = - \begin{pmatrix} 1 & -m_{12} \\ 0 & 1 \end{pmatrix} = -I_2 T^{-m_{12}} = S^2 T^{-m_{12}}$$

d'où $M \in \langle S, T \rangle$.

On a bien prouvé que si $\mu(M) = 0$, alors $M \in \langle S, T \rangle$.

- (b) On calcule, pour tout $k \in \mathbb{Z}$, $ST^k = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ puis

$$ST^k M = \begin{pmatrix} -m_{21} & -m_{22} \\ m_{11} + km_{21} & m_{12} + km_{22} \end{pmatrix}$$

Par conséquent, pour tout $k \in \mathbb{Z}$, $\mu(ST^k M) = |m_{11} + km_{21}|$. Par ailleurs,

$$\begin{aligned} |m_{11} + km_{21}| < |m_{21}| &\Leftrightarrow -|m_{21}| < m_{11} + km_{21} < |m_{21}| \\ &\Leftrightarrow -m_{11} - |m_{21}| < km_{21} < -m_{11} + |m_{21}| \end{aligned}$$

Or l'intervalle $] -m_{11} - |m_{21}|, -m_{11} + |m_{21}|[$ est de largeur $2|m_{21}|$: par conséquent il contient un multiple de m_{21} . Soit donc $k \in \mathbb{Z}$ tel que km_{21} appartienne à cet intervalle. On a alors $|m_{11} + km_{21}| < |m_{21}|$, autrement dit $\mu(ST^k M) < \mu(M)$.

- (c) D'après ce qui précède, si $\mu(M) > 0$, alors il existe $k_1 \in \mathbb{Z}$ tel que $\mu(ST^{k_1} M) < \mu(M)$. Posons $M_1 = ST^{k_1} M \in SL_2(\mathbb{Z})$. Si $\mu(M_1) > 0$, il existe alors k_2 tel que $\mu(ST^{k_2} M_1) < \mu(M_1) < \mu(M)$. On peut répéter le processus tant que $\mu(M_j) > 0$. On construit ainsi une suite d'entiers k_1, \dots, k_n et une suite de matrices M_1, \dots, M_n tels que $M_j = ST^{k_j} M_{j-1}$ et $\mu(M_j) < \mu(M_{j-1})$ pour tout $j \geq 1$ (en posant $M_0 = M$). La suite $(\mu(M_j))_{j \geq 0}$ est une suite strictement décroissante d'entiers naturels : par conséquent il existe $n \in \mathbb{N}$ tel que $\mu(M_n) = 0$.

D'après la question précédente, il existe alors $p \in \mathbb{Z}$ tel que $M_n = S^2 T^p$. Mais $M_n = ST^{k_n} M_{n-1} = ST^{k_n} ST^{k_{n-1}} M_{n-2} = ST^{k_n} \dots ST^{k_1} M_0$.

Par conséquent, $M = M_0 = T^{-k_1} S^{-1} \dots T^{-k_n} S^{-1} S^2 T^p$ ce qui prouve que $M \in \langle S, T \rangle$. On a bien prouvé que dans tous les cas, $M \in \langle S, T \rangle$. Ainsi $SL_2(\mathbb{Z}) \subset \langle S, T \rangle$. Mais l'inclusion réciproque est vraie également puisque $S \in SL_2(\mathbb{Z})$, $T \in SL_2(\mathbb{Z})$ et $SL_2(\mathbb{Z})$ est un groupe. Par conséquent, $SL_2(\mathbb{Z}) = \langle S, T \rangle$.

- (d) Les coefficients de A sont entiers et $\det(A) = -9 \times (-1) - 4 \times 2 = 1$ donc $A \in SL_2(\mathbb{Z})$. De plus, on a $\mu(A) = 4 > 0$, $-a_{11} - |a_{21}| = 9 - 4 = 5$, $-a_{11} + |a_{21}| = 9 + 4 = 13$. Et l'intervalle $]5, 13[$ contient $8 = 2 \times 4$. Posons alors

$$A' = ST^2 A = \begin{pmatrix} -4 & 1 \\ -1 & 0 \end{pmatrix}$$

On a bien $A' \in SL_2(\mathbb{Z})$ et $\mu(A') < \mu(A)$. De plus, $\mu(A') = 1 > 0$, il est donc nécessaire de réitérer l'opération.

On a $-a'_{11} - |a'_{21}| = 4 - 1 = 3$, $-a'_{11} + |a'_{21}| = 4 + 1 = 5$ et l'intervalle $]3, 5[$ contient $4 = (-4) \times (-1)$.

Posons $A'' = ST^{-4} A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. On a donc $ST^{-4} ST^2 A = I_2$ d'où $A = T^{-2} S^{-1} T^4 S^{-1}$.

III. Ordre des éléments de $SL_2(\mathbb{Z})$

11. • On a $I_2^1 = I_2$ donc I_2 est d'ordre fini et son ordre vaut 1.
• On a $S^4 = I_2$ donc S est d'ordre fini.
Comme on a vu que $S \neq I_2$, $S^2 \neq I_2$, $S^3 \neq I_2$, l'ordre de S est égal à 4.

• Calculons :

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad (ST)^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad (ST)^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

On remarque que $(ST)^3 = -I_2$.

Par conséquent $(ST)^6 = (-I_2)^2 = I_2$ et ST est d'ordre fini.

De plus, $(ST)^4 = (ST)(ST)^3 = (ST)(-I_2) = -ST \neq I_2$ et

$(ST)^5 = (ST)^2 (ST)^3 = (ST)^2 (-I_2) = -(ST)^2 \neq I_2$.

On en déduit que l'ordre de ST vaut 6.

- D'après ce qui précède, $((ST)^2)^3 = (ST)^6 = I_2$ donc $(ST)^2$ est d'ordre fini. De plus, $(ST)^2 \neq I_2$ et $((ST)^2)^2 = (ST)^4 \neq I_2$, donc $(ST)^2$ est d'ordre 3.

12. Soit $M \in GL_2(\mathbb{R})$ d'ordre fini, soit $p \in \mathbb{N}^*$ tel que $M^p = I_2$.

Alors $(M^2)^p = M^p M^p = I_2 I_2 = I_2$ donc M^2 est d'ordre fini.

13. (a) On a $M^2 - \text{tr}(M)M + \det(M)I_2 = 0$ d'où pour tout $k \in \mathbb{N}$,
 $M^{k+2} - \text{tr}(M)M^{k+1} + \det(M)M^k = 0$.

Il s'ensuit, par linéarité de la trace, $u_{k+2} - \text{tr}(M)u_{k+1} + \det(M)u_k = 0$.

- (b) Supposons $|\text{tr}(M)| \geq 3$. L'équation caractéristique de la relation de récurrence est $r^2 - \text{tr}(M)r + \det(M) = 0$.

Son discriminant vaut $\Delta = \text{tr}(M)^2 - 4\det(M) = \text{tr}(M)^2 - 4$ puisque $\det(M) = 1$. Or, par croissance de la fonction carré sur \mathbb{R}_+ , $\text{tr}(M)^2 \geq 9$ donc $\Delta > 0$. L'équation caractéristique possède donc deux racines

$$r_1 = \frac{\text{tr}(M) - \sqrt{\text{tr}(M)^2 - 4}}{2} \quad \text{et} \quad r_2 = \frac{\text{tr}(M) + \sqrt{\text{tr}(M)^2 - 4}}{2}$$

Il existe donc α et $\beta \in \mathbb{R}$ tels que pour tout $k \in \mathbb{N}$, $u_k = \alpha r_1^k + \beta r_2^k$.

De plus, $u_0 = \text{tr}(I_2) = 2 = \alpha + \beta$ et $u_1 = \text{tr}(M) = \alpha r_1 + \beta r_2$.

Résolvons le système linéaire

$$\begin{cases} \alpha + \beta = 2 \\ \alpha r_1 + \beta r_2 = \text{tr}(M) \end{cases}$$

$L_2 - r_1 L_1$ donne $\beta(r_2 - r_1) = \text{tr}(M) - 2r_1 = \sqrt{\text{tr}(M)^2 - 4}$.

Or $r_2 - r_1 = \sqrt{\text{tr}(M)^2 - 4}$, on en déduit donc $\beta = 1$.

Par suite, $\alpha = 2 - \beta = 1$. Ainsi, pour tout $k \in \mathbb{N}$, $u_k = r_1^k + r_2^k$ soit

$$u_k = \left(\frac{\text{tr}(M) - \sqrt{\text{tr}(M)^2 - 4}}{2} \right)^k + \left(\frac{\text{tr}(M) + \sqrt{\text{tr}(M)^2 - 4}}{2} \right)^k$$

Or $\text{tr}(M)^2 \geq 9$ donc par croissance de la fonction racine carrée, $\sqrt{\text{tr}(M)^2 - 4} \geq \sqrt{5}$. Distinguons deux cas :

- Si $\text{tr}(M) \geq 3 > \sqrt{5}$ alors $r_1 > 0$ et $r_2 > 1$, par conséquent $|u_k| = u_k$ pour tout $k \in \mathbb{N}$ et $\lim_{k \rightarrow +\infty} |u_k| = +\infty$.
- Si $\text{tr}(M) \leq -3 < -\sqrt{5}$ alors $r_1 < -1$ et $r_2 < 0$. Par conséquent, r_1^k et r_2^k sont de même signe pour tout $k \in \mathbb{N}$ et $|u_k| = |r_1|^k + |r_2|^k$. Comme $|r_1| > 1$, on en déduit $\lim_{k \rightarrow +\infty} |u_k| = +\infty$.

14. (a) Notons $p \in \mathbb{N}^*$ l'ordre de M . Ainsi $M^p = I_2$. On en déduit que pour tout $k \in \mathbb{N}^*$, $M^{kp} = I_2$ et $\text{tr}(M^{kp}) = \text{tr}(I_2) = 2$.

Par l'absurde, si $|\text{tr}(M)| \geq 3$, d'après ce qui précède on a $\text{tr}(M^k) \xrightarrow{k \rightarrow +\infty} 0$, contradiction. Donc $|\text{tr}(M)| < 3$, et comme $\text{tr}(M) \in \mathbb{Z}$, $|\text{tr}(M)| \leq 2$.

(b) Supposons $\text{tr}(M) = -1$. On a donc $M \neq I_2$ puisque $\text{tr}(I_2) = 2$.

En outre, $M^2 = \text{tr}(M)M - \det(M)I_2 = -M - I_2 \neq I_2$ puisque $\text{tr}(M^2) = -\text{tr}(M) - \text{tr}(I_2) = -(-1) - 2 = -1 \neq 2 = \text{tr}(I_2)$.

On en déduit enfin $M^3 = -M^2 - M = -(-M - I_2) - M = I_2$, ce qui montre que M est d'ordre 3.

(c) Supposons $\text{tr}(M) = 1$. Alors $M^2 = \text{tr}(M)M - \det(M)I_2 = M - I_2$, et $\text{tr}(M^2) = \text{tr}(M) - \text{tr}(I_2) = 1 - 2 = -1$. De plus, M^2 est d'ordre fini et d'après la question précédente on a $M^6 = (M^2)^3 = I_2$.

En outre, $M^3 = M(M - I_2) = M^2 - M = (M - I_2) - M = -I_2 \neq I_2$, d'où $M^4 = -M \neq I_2$ et $M^5 = -M^2 = I_2 - M \neq I_2$. Par conséquent M est d'ordre 6.

(d) Prouvons par récurrence que pour tout $k \in \mathbb{N}^*$, il existe $Q_k \in \mathcal{M}_2(\mathbb{R})$ telle que $M^k = I_2 + k(M - I_2) + (M - I_2)^2 Q_k$.

- On a $M^1 = I_2 + (M - I_2) + (M - I_2)^2 O$ donc la propriété est vraie pour $k = 1$ avec $Q_1 = O$.
- On a $M^2 = I_2 + 2(M - I_2) + (M - I_2)^2$ donc la propriété est vraie pour $k = 2$ avec $Q_2 = I_2$.
- Soit $k \in \mathbb{N}^*$ tel que la propriété soit vraie. Calculons alors

$$\begin{aligned} M^{k+1} &= MM^k \\ &= M(I_2 + k(M - I_2) + (M - I_2)^2 Q_k) \quad (\text{hyp. de récurrence}) \\ &= M + k(M^2 - M) + M(M - I_2)^2 Q_k \\ &= M + k(I_2 + 2(M - I_2) + (M - I_2)^2 - M) + M(M - I_2)^2 Q_k \\ &= M + k(M - I_2 + (M - I_2)^2) + M(M - I_2)^2 Q_k \\ &= M + k(M - I_2) + k(M - I_2)^2 + M(M - I_2)^2 Q_k \\ M^{k+1} &= I_2 + (k + 1)(M - I_2) + (M - I_2)^2 (kI_2 + MQ_k) \end{aligned}$$

la dernière égalité étant permise par le fait que M commute avec la matrice $(M - I_2)^2$. Ainsi, si on pose $Q_{k+1} = kI_2 + MQ_k \in \mathcal{M}_2(\mathbb{R})$, on a bien $M^{k+1} = I_2 + (k + 1)(M - I_2) + (M - I_2)^2 Q_{k+1}$ et la propriété est vraie pour $k + 1$.

Ainsi par récurrence, pour tout $k \in \mathbb{N}^*$, il existe $Q_k \in \mathcal{M}_2(\mathbb{R})$ telle que $M^k = I_2 + k(M - I_2) + (M - I_2)^2 Q_k$.

(e) Supposons $\text{tr}(M) = 2$.

Écrivons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ainsi $M - I_2 = \begin{pmatrix} a - 1 & b \\ c & d - 1 \end{pmatrix}$ et

$$\begin{aligned} \det(M - I_2) &= (a - 1)(d - 1) - bc \\ &= ad - bc - (a + d) + 1 \\ &= \det(M) - \text{tr}(M) + 1 \\ \det(M - I_2) &= 1 - 2 + 1 = 0 \end{aligned}$$

En outre, $\text{tr}(M - I_2) = \text{tr}(M) - \text{tr}(I_2) = 2 - 2 = 0$.

On en déduit $(M - I_2)^2 = \text{tr}(M - I_2)(M - I_2) - \det(M - I_2)I_2 = O$.

Par ailleurs, comme M est d'ordre fini, il existe un entier $p \in \mathbb{N}^*$ tel que $M^p = I_2$. Mais d'après le résultat précédent,

$M^p = I_2 + p(M - I_2) + (M - I_2)^2 Q_p$ soit $I_2 = I_2 + p(M - I_2)$ ou encore $p(M - I_2) = 0$. Comme $p \neq 0$, on en déduit enfin $M = I_2$ et M est d'ordre 1.

(f) On a vu que si $\text{tr}(M) \in \{-1, 1, 2\}$ alors l'ordre de M appartient à $\{1, 3, 6\}$. Il reste à traiter les cas $\text{tr}(M) = -2$ et $\text{tr}(M) = 0$.

- Si $\text{tr}(M) = -2$, alors $-M \in SL_2(\mathbb{Z})$, $-M$ est d'ordre fini et en outre, $\text{tr}(-M) = -\text{tr}(M) = 2$. D'après ce qui précède, $-M = I_2$ donc $M = -I_2$ et M est d'ordre 2.
- Si $\text{tr}(M) = 0$, alors $M \neq I_2$ et $M^2 = \text{tr}(M)M - \det(M)I_2 = -I_2$. On en déduit $M^3 = -M \neq I_2$ et $M^4 = I_2$. Par conséquent M est d'ordre 4.

On a donc montré que l'ordre de M appartient à $\{1, 2, 3, 4, 6\}$.